Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: www.tandfonline.com/journals/tbit20

Unpacking creepiness: a study on smart home sensor surveillance

Sujay Shalawadi, Dimitrios Raptis & Florian Echtler

To cite this article: Sujay Shalawadi, Dimitrios Raptis & Florian Echtler (12 Dec 2025): Unpacking creepiness: a study on smart home sensor surveillance, Behaviour & Information Technology, DOI: 10.1080/0144929X.2025.2598603

To link to this article: https://doi.org/10.1080/0144929X.2025.2598603

Published online: 12 Dec 2025.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2025.2598603

Taylor & Francis
Taylor & Francis Group

Unpacking creepiness: a study on smart home sensor surveillance

Sujay Shalawadi [a], Dimitrios Raptis [b] and Florian Echtler [b]

[a]Department of Design, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway; [b]Human-Centered Computing, Department of Computer Science, Aalborg University, Aalborg, Denmark

ABSTRACT

The paper investigates the subjective experience of creepiness in smart home devices, focussing on privacy concerns surrounding unauthorised data access, invasive personalisation, and covert surveillance. The study consisted of scenario development and validation followed by semi-structured interviews. Findings reveal how users perceive smart home interactions as increasingly intrusive, particularly in relation to the temporality of data management where non-consensual targeted advertisements based on recent activities contribute to heightened discomfort. Key findings show that perceptions of creepiness are highly individual, shaped by users' past experiences and expectations of technology. Despite recognising privacy risks, participants often prioritise the convenience these devices offer, leading to a paradox where users continue to engage with technologies that make them feel uncomfortable. We highlight the need for designers to implement hybrid privacy solutions that combine manual and automated controls to help users manage their privacy settings more effectively. By offering real-time notifications, increasing transparency in data collection practices, and making privacy controls more accessible, designers can mitigate the normalisation of perceived creepiness associated with smart home devices. This study contributes to the broader conversation on affective privacy, emphasising the emotional impact of smart home surveillance on users and providing insights for more privacy-conscious design strategies.

ARTICLE HISTORY
Received 13 January 2024
Accepted 23 November 2025

KEYWORDS
Smart home sensors; surveillance; privacy; creepiness; interactive systems and tools

1. Introduction

The increasing integration of smart home devices has significantly altered the dynamics of domestic privacy (Geeng and Roesner 2019; Koshy et al. 2021). Devices such as smart speakers, cameras, and motion sensors have become commonplace in households, offering convenience, security, and enhanced control over home environments. Device manufacturers promise to make our lives easier by automating daily tasks, monitoring security, and providing personalised experiences through their products (Huberman 2021). However, the rapid adoption of these smart home devices has raised significant concerns about privacy intrusions (Pierce 2019b; Pierce, Wong, and Merrill 2020; Shalawadi et al. 2024). Users are increasingly aware of the potential for these devices to continuously monitor their activities, often without clear consent or understanding of how their data is used (Knijnenburg et al. 2022; Thakkar et al. 2022).

As we use more smart home devices, it is getting harder for people to know which information will stay private and which might be shared with companies or third parties (Knijnenburg et al. 2022; Tabassum, Kosinski, and Lipford 2019; Wellendorf, Søilen, and Veel 2022). This intrusion has led to a growing sense of unease, often described as 'creepiness' (Raff, Rose, and Huynh 2024; Vitak 2020). This feeling of creepiness arises not only from the perceived invasion of privacy but also from the unpredictability and opacity of these technologies (Pierce, Wong, and Merrill 2020). In general, users may not fully understand when they are being watched or how their data is being processed and shared, leading to discomfort and mistrust (Phelan, Lampe, and Resnick 2016; Woźniak et al. 2021).

Existing research has highlighted significant gaps in understanding the emotional and psychological responses to creepiness felt due to covert surveillance mechanisms of technologies (Seberger et al. 2022; Woźniak et al. 2021). This is also evident with privacy studies in the context of smart homes (Shalawadi et al. 2024; Wong et al. 2023). Although privacy concerns have been extensively studied, the specific experience of creepiness, characterised by visceral, often irrational discomfort, remains underexplored (Knijnenburg et al.

CONTACT Sujay Shalawadi sujay.shalawadi@ntnu.no Raufossvegen 40, 2821 Gjøvik, Norway

2022; Woźniak et al. 2021). Previous studies have noted that users often continue to engage with smart home technologies despite expressing significant privacy concerns, a paradox that suggests a deeper understanding of the unresolved tension between the benefits of these technologies and the discomfort they provoke (Hanson et al. 2020; Lau, Zimmerman, and Schaub 2018; Seberger et al. 2022; Vitak 2020).

Therefore, in this paper, our aim is to explore perceived creepiness in the context of smart home sensor surveillance. In particular, we seek to answer two research questions:(1) How do users experience and rationalise the feeling of creepiness in relation to smart home devices?, and (2) What factors contribute most significantly to these perceptions? To explore this, we conducted semi-structured interviews with 16 users of various smart home devices, using tailored scenarios that highlight common privacy-convenience trade-offs, and analysed their emotional responses to these surveillance situations.

The key findings of this study highlight the widespread sense of discomfort - often described as creepiness – associated with smart home sensor surveillance. Participants expressed persistent privacy fears, particularly about unauthorised data access and the hidden data practices of smart home devices. The creepiness was intensified by the awareness of constant surveillance, the potential for biased or manipulative content, and the lack of transparency in how data is collected and used. Interestingly, despite recognising these privacy intrusions, many participants continued to use smart home technologies, rationalising the trade-off between convenience and privacy. The study also found that creepiness was influenced by the temporal proximity of data usage to recent activities, as well as by the context and subjectivity of individual users.

The contributions of this paper are threefold. First, we provide a detailed examination of the subjective experience of creepiness in smart home sensor surveillance, highlighting how users' emotional reactions to creepy experiences with smart home devices vary based on personal experiences and expectations, demonstrating that creepiness is highly individualised. Second, we identify key factors that influence creepiness, emphasising the importance of temporality in privacy perceptions. Users particularly perceive high creepiness from targeted ads based on recent activities, underscoring the need for timely transparency in data use. While convenience is often prioritised, the discomfort tied to real time exploitation of personal data for company economics remains a significant concern. Third, we propose design strategies to mitigate creepiness, focussing on enhancing user control and transparency through real time notifications and hybrid privacy solutions that empower users to manage their privacy more effectively, reducing discomfort and privacy cynicism.

In the following sections, we situate our approach to studying perceived creepiness in the relevant literature. We then describe our methodology by describing how we developed and validated scenarios for the semi-structured interviews. Subsequently, we present the findings of our semi-structured interviews as five themes. We proceed to discuss the findings in depth by providing implications on how to better preserving end-user privacy with smart home devices.

2. Related work

In this section, we examine the evolution of privacy concerns in smart homes and their impact on users. Specifically, we review previous work on perceived creepiness and discomfort arising from these privacy issues. We conclude by exploring how others have attempted to address creepiness and identify the research gaps that our study aims to fill.

2.1. The evolution of privacy concerns in smart homes

The Aware Home Research Initiative, established in the late 1990s, aimed to enhance independent living through innovative technologies while emphasising privacy and simplicity (Kientz et al. 2008). This early vision envisioned a closed-loop system under the control of its occupants, focussing on user autonomy. However, the introduction of commercial smart home devices has significantly transformed this landscape, integrating complex data collection practices into the broader data economy (Sadowski 2020; Stark and Levy 2018). Social psychologist Shoshana Zuboff raises important concerns about how companies exploit the vast data generated by smart devices, emphasising the power imbalances that favour corporations over end-users and intensifying privacy concerns (Zuboff 2019).

Traditional ideas of privacy emphasise an individual's control over personal information, the protection of private spaces, and the ability to maintain anonymity without constant surveillance (Solove 2002; Westin 1968). However, the shift from privacy-focussed initiatives, like the Aware Home Research Project, to commercially driven smart home devices has introduced complex data collection practices that challenge these notions of privacy (Apthorpe et al. 2022; Tabassum, Kosinski, and Lipford 2019). Users now face reduced control and transparency regarding how their data is collected and used, making it harder to maintain

traditional privacy expectations in a digital world of constant monitoring and pervasive smart technologies (Acquisti and Grossklags 2005). In the domain of smart homes, the shift towards commercial profitability by manufacturers has intensified disparities between household users, often attracting more technically proficient users over those less familiar with technology (Geeng and Roesner 2019; Koshy et al. 2021). Studies indicate that while users initially experience discomfort from constant surveillance, they engage in privacy-seeking behaviours. However, over time, this surveillance becomes normalised, integrated into daily life, and perceived as background, resulting in no significant long-term increase in stress (Oulasvirta et al. 2012).

Recent meta-analytic work by Kim et al. (2023) consolidates findings from over 180 studies and confirms the persistent disconnect between privacy concern and actual behaviour, a phenomenon commonly described as the privacy paradox. While their analysis shows that privacy concern significantly predicts protection intentions more than actual protective behaviour, it also highlights the influence of contextual and methodological factors, such as culture and measurement tools. Building on this, our study explores how affective experiences like discomfort, unease, and creepiness further nuance this paradox in smart home environments, where surveillance is not only invisible and constant but also occurs within the spaces users associate with safety and routine.

2.2. Navigating the creepiness factor in smart homes

As smart home technologies evolve, they often disrupt established social norms, leading to discomfort, commonly referred to as 'creepiness' (Raff, Rose, and Huynh 2024; Vitak 2020). This discomfort is closely tied to privacy concerns, as users frequently experience a loss of control when technology behaves unpredictably or fails to meet expectations (Do et al. 2023; Seberger et al. 2022). Studies by Zeng, Mare, and Roesner (2017) and Zimmermann et al. (2019) explore how different sensors like cameras, motion detectors, and voice assistants contribute to these feelings of unease, especially within the domestic setting where surveillance is ambient, continuous, and often hidden in everyday routines. Zeng, Mare, and Roesner (2017) in particular show how smart home surveillance differs from online privacy threats by emphasising the invisible nature of in-home monitoring, where users are often unsure when, how, and why data is being collected,an aspect that profoundly shapes affective discomfort.

Wong et al. (2023) further emphasises the ethical and social implications, particularly how these devices can create power imbalances, leading to heightened perceptions of creepiness. Although previous studies have explored how sensors like cameras and voice assistants contribute to discomfort and examined ethical implications, more research is needed to understand how specific device features, such as targeted advertisements, exacerbate privacy concerns.

Lau, Zimmerman, and Schaub (2018) examine how the continuous listening capability of smart speakers amplifies privacy concerns, particularly when users and bystanders are uncertain about what is being recorded and how that data might be used. This highlights the importance of understanding how disruptions to social norms contribute to emotional reactions that reinforce the need to unpack the notion of creepiness in smart home environments. Seymour et al. (2023) highlight how voice assistant devices disrupt social norms by perpetuating gender stereotypes and enabling constant surveillance.

Moreover, Knijnenburg et al. (2022) discuss the paradox of users continuing to engage with smart home technologies despite significant privacy concerns. These concerns warrant further exploration as smart home devices blur the distinction between private and public spaces. By collecting data within the home,traditionally seen as private,these devices create uncertainty about the boundaries of personal information, heightening feelings of discomfort or creepiness. Lenhart et al. (2023) have also studied that despite being technically proficient, these users find managing privacy within the smart home ecosystem complex and often confusing. Thakkar et al. (2022) emphasise that the opaque data practices of smart home devices, especially the lack of transparency in data collection and sharing, significantly contribute to discomfort or creepiness, particularly for bystanders who may unknowingly be subject to surveillance. Yao et al. (2023) highlight the crucial role of human-centered research, with a specific focus on user experience, privacy, and security. Their work underscores that many smart home devices fail to fully grasp user discomfort, privacy concerns, and the emotional responses that these devices can provoke. Park et al. (2023) highlight the privacy concerns of smart home primary users, emphasising their dissatisfaction with current data transparency, visibility, and control options. The paper proposes design improvements to balance privacy, usability, and customisation, advocating for more user-friendly privacy controls applicable to both technical and non-technical users. Meng-Schneider et al. (2023) show the lack of transparency in how smart speakers handle data and their ability to listen to conversations without clear user control

can evoke feelings of being constantly watched or monitored, contributing to perceptions of creepiness.

Recent work by Shalawadi, Echtler, and Raptis (2024) highlights the psychological and affective dimensions of continued voice assistant use, revealing how users rationalise their privacy concerns through apathy and justification mechanisms. Their study, which combines interviews with a provotypical intervention, provides design implications for breaking apathetic privacy attitudes,a theme that resonates with our exploration of emotional responses like creepiness and the persistent use of smart home devices despite discomfort.

Based on the literature, we observe that while smart home devices often favour primary users over secondary ones, primary users are also frustrated by the complexity of managing privacy due to the opaque nature of data handling by smart home companies. This situation motivates our study to explore the perception of creepiness linked to privacy risks in smart homes, with the goal of proposing more user-friendly privacy controls and greater transparency in data management.

2.3. Addressing the need for transparency and control

The notion of creepiness' in smart homes is often linked to technologies that continuously track personal data, raising privacy concerns due to unclear data handling and perceived lack of control (Nadon et al. 2018; Ngo and Krämer 2022). Seberger et al. (2022) show how affective discomfort (emotional reactions like unease or creepiness) is becoming normalised in app use, even when privacy violations are perceived. Creepiness is particularly evident in scenarios involving leaky sensors' on devices like cameras, where digital information can be shared or misused by adversaries without the individual's knowledge, causing significant discomfort (Pierce, Wong, and Merrill 2020; Tan, Wong, et al. 2022). Pierce (2019b) highlight the need to address evolving social norms regarding acceptable behaviours of smart home devices in private spaces. As smart home technologies become more widespread, societal tolerance for privacy and surveillance concerns may shift, especially as devices with hidden functionalities, which operate without user knowledge, raise ethical questions. In this regard, Windl, Schmidt, and Feger (2023) emphasise the importance of tangible privacy mechanisms that offer users control over individual sensors, such as cameras and microphones, while providing clear feedback on data collection practices. Similarly, Shalawadi et al. (2024) recommend integrating physical privacy controls in smart home camera designs to enhance user-friendly privacy mechanisms and propose design recommendations to balance privacy concerns with the convenience of constant surveillance.

Phelan, Lampe, and Resnick (2016) illustrates how users often feel an intuitive sense of discomfort, commonly described as 'creepy' when interacting with technologies that invade their privacy. However, this emotional response does not always lead to behavioural changes, as users can rationalise the risks as minor compared to the benefits they receive from technology (Chalhoub et al. 2020; Zheng et al. 2018). This discrepancy between how users feel (creepiness) and how they act (continued use despite discomfort) underscores the importance of addressing the emotional side of privacy concerns. Lau, Zimmerman, and Schaub (2018) illustrate how misaligned privacy controls exacerbate feelings of creepiness, with user often finding these controls underutilised or misunderstood, leading to greater discomfort and distrust. Previous studies (Thakkar et al. 2022; Vitak 2020; Windl, Schmidt, and Feger 2023) emphasise that opaque data practices contribute significantly to discomfort, particularly for bystanders. Addressing these issues is critical for reducing the emotional and psychological burden associated with smart home technologies.

3. Method

We decided to select semi-structured interviews for deeply exploring participants' affective and contextual responses to smart home surveillance. This method was particularly suited to capturing nuanced emotional states of perceived creepiness which are often difficult to elicit through surveys or focus groups. Interviews also enabled participants to reflect on personal, situated experiences in their domestic spaces, which are essential when examining ambient and often invisible surveillance.

Our study aims to understand the factors that trigger creepiness in smart home technologies and suggest ways to reduce them. In doing this, our goal is to contribute to the way smart home devices make users feel safe and secure, which will improve their overall trust and acceptance of the technology. To achieve this goal, we conducted semi-structured interviews with 16 participants, using scenarios as a tool to encourage participants to narrate their own perceived creepy experiences using their own devices. In the following, we provide a detailed overview of our study design, comprising two main components: (A) scenario construction and (B) semi-structured interviews.

3.1. Part A: scenario construction and validation

3.1.1. Scenario construction

Building on previous research on creepiness (Seberger et al. 2021; Shklovski et al. 2014), which highlighted

the tendency of people to feel guilty when discussing privacy violations and their corresponding actions, we recognised the potential pitfalls of direct privacy inquiries, as they may lead to inflated expressions of privacy concerns (Braunstein, Granka, and Staddon 2011). In response to these challenges, we devised a set of scenarios to serve as a tool, prompting participants to openly share their personal experiences with creepiness.

Scenario-based methodologies have gained significant traction in the broader landscape of creepiness and privacy-related research, finding application in diverse domains such as smartphone apps, social networking sites, and attitudes toward automated gender recognition, as demonstrated in prior studies (Enck et al. 2014; Seberger et al. 2021, 2022; Shvartzshnaider et al. 2016). When constructing these scenarios, our approach to understanding creepiness drew inspiration from the conceptual framework put forth by Woźniak et al. (2021). This comprehensive framework considers three key factors that collectively encapsulate the essence of creepiness.

(1) *Implied Malice*: This factor relates to the perception of bad intentions conveyed through the design of the technology.
(2) *Undesirability*: This factor pertains to the interactive artifact being perceived as out of context.
(3) *Unpredictability*: This factor involves negative feelings stemming from users' inability to anticipate the actions of interactive technologies and their difficulty in exerting the desired level of control.

Since we relied on the conceptualisation of creepiness from the framework of Woźniak et al. (2021), we made sure to include the above three factors when developing each scenario. In-depth descriptions of these scenarios are available in Table 1. The choice of smart home sensors and devices along with the conveniences they offer users was inspired by ongoing technology debates widely covered in the media that included self-reported privacy violation experiences from active smart home users and blogs written by free-lance technology critics. The smart home sensors and devices that were finally included were motivated by the votes of people on the question that Mozilla asked users: *How creepy do you think this is?* on the public forum 'privacy not included' from Mozilla foundation (Mozilla Foundation n.d.).

To illustrate the creepiness conceptualisation of Woźniak et al. (2021), consider Scenario 2, named 'Hands-Free'. In this scenario, we outline typical user expectations by presenting a familiar voice-activated, hands-free interaction through the audio sensor embedded in a voice assistant. The scenario sets the stage for users to seamlessly enjoy music without any hassle, a convenience that enhances their daily lives. However, this convenience collides head-on with the device's 'always-on' recording mode and its opaque

Table 1. Scenarios arranged in descending order of perceived creepiness that were used in semi-structured interviews.

Scenario Text
Video Call (Camera)
You have a video assistant similar to a voice assistant that can allow you to make video calls. Similarly to voice assistants, you can also use a wake word and ask the video assistant to call people from your contact list, which automatically syncs once you have signed up with your email ID. After a few days of use, you notice while scrolling through your social media feed that the video assistant company has used a screenshot of one of your calls with your close friend to advertise their product. You have no way of challenging the use of the photo in the ad.
Hands-Free (Audio)
You have a voice assistant that you use to play music at home. The device is ready to play your favourite music once it hears the wake word. Lately you have been having arguments with your significant other. After a few days, you and your partner start hearing advertisements about couple counselling periodically when trying to play your music. You could disable the ads for a monthly subscription fee.
Cleaning (Camera)
You have a robot vacuum cleaner that works with your voice assistant for hands-free control. The robot vacuum cleaner has a high-definition camera that captures your house at low angle so it can clean the floor and avoid obstacles. Your friend recently told you about the vacuum cleaning company sending the data collected halfway across the world, where the company hires people to manually go through the recordings to look for potential advertising that can be targeted to you via other third party companies. You can opt out of getting the advertisements, but this would reduce the functionality of the robot vacuum.
Media Aggregator (Audio) You have a smart TV that helps you stream content from the Internet for entertainment. Recently, you have cast your vote for a different political party for the first time after many years and have mentioned this briefly to your close friends and family. Your smart TV dashboard often starts showing documentaries related to the ideologies of the political party. Your friends who use similar smart TVs barely see anything from that political party.
Smart Scale (WiFi)
You have bought a smart scale that can help you stay informed about various body markers like body fat percentage. The company recommends that you provide your personal information, such as date of birth and sex, to provide accurate readings of body markers. You can also opt not to provide personal information and interpret the body marking yourself. Recently, you read an article that the company sells your body markers like weight and height along with personal information to third parties who can then provide personalised advertisements on gym memberships or low-calorie food.
Smart Groceries (RFID)
You have bought a smart refrigerator that is connected to your voice assistant. The refrigerator keeps track of what is being put in by scanning the products. The voice assistant can then tell you verbally if you are running low on food supplies. A few days later, a friend tells you that the smart refrigerator company shares your scanned food supplies data with the local supermarket chains. You can select which supermarket chains will receive your data.
Smart Heating (Location)
Your home is equipped with a smart thermostat that senses when you enter the room physically and sets the temperature accordingly. You have done this so that the smart thermostat can better recognise your presence and set the temperature appropriately. For the sensor to function well, the smart thermostat must remain connected to the cloud servers of the firm with your log-in account. When connected to your smartphone app, the smart thermostat can determine your location when you are away from the house. The smart thermostat can then estimate your distance from home and turn on/off your heating accordingly. You can opt out of using the smartphone app but could miss software updates and temperature control prior to your arrival home.

data management practices (implied malice). This lack of transparency (unpredictability) culminates in the delivery of targeted advertisements, a development that can cause feelings of creepiness among users. Their negative emotions arise from their unawareness of the data source used to fuel these advertisements (undesirability).

3.1.2. Scenario validation procedure

We conducted an online survey to explicitly validate that the seven scenarios exhibited diverse levels of creepiness, as defined by the three creepiness factors outlined in the framework by Woźniak et al. (2021). To ensure this variation, we used a pre-validated tool, the 'Perceived Creepiness Technology Scale' (Woźniak et al. 2021), based on the same conceptual framework. This validation process was crucial in confirming that each scenario varied in intensity of creepiness, thereby stimulating a range of emotional responses during the interviews.

We recruited 126 participants through the Prolific crowd-sourcing platform, specifically selecting individuals with a proven acceptance rate of 95% or higher in previous crowd-working engagements. We ensured that our survey adhered to the ethical guidelines established by our Institutional Review Board. To ensure relevance, we filtered participants based on their use of specific smart home devices featured in our scenarios. Compensation adhered to UK minimum wage guidelines, offering £10.42 per hour, with a reward of £1.9 for each participant for completing the 10-minute survey. The questionnaire was designed using Qualtrics. To minimise cognitive burden and improve the reliability of responses, each participant was shown only one of the seven scenarios. We used a randomised Latin Square design to ensure equal distribution, with each scenario being presented to exactly 18 of the 126 participants. This approach ensured that all scenarios were represented evenly across the sample. Based on the scenario presented, each participant rated their perceived creepiness. We used the 'Smart Home Privacy Concern Scale' by Guhr et al. (2020) before presenting the scenarios as a starting point to measure participants' existing privacy concerns. Moreover, in relation to our objective of understanding perceived creepiness in smart home sensor surveillance, key privacy dimensions of the privacy scale, such as data tracking, surveillance, and intrusion, are related to feelings of creepiness. Furthermore, we expected the score distribution to be normal, ensuring the participant sample was representative of a broad range of privacy concerns.

The ages of the participants ranged from 19 to 59 years, averaging 28.5 years (SD = 8.7), and identified gender distribution was even (Men = 63, Women = 63). The sample consisted of individuals of 21 nationalities in six geographical regions. Asia (60), Africa (20), Europe (15), North America (17), South America (8) and Oceania (6). Household occupancy varied: Alone (9), staying with partner (28), staying with family including partner and children (30), staying with family including partner, parents, and children (44), and staying in a joint family (15). Educational qualifications included discontinued high school (4), high school (30), Bachelor's degree (55), Master's degree (33), and Ph.D. or higher (4). All participants had been using their smart home devices for at least 3 months.

Our participant sample had an average privacy concern score of 41 (SD = 6.9) out of a maximum possible score of 55. Among the 126 valid responses, the privacy concern scores were normally distributed according to a Shapiro-Wilk test ($W = 0.986$, $p = 0.2168$). This confirms that most participants had scores around the average (41), with fewer participants having very high or very low scores. The video call scenario was rated as the most creepy, while the smart heating scenario was considered the least creepy.

3.2. Part B: interview study

We conducted semi-structured interviews with 16 participants using the scenarios developed to explore their psychological responses to creepy experiences. The interviews aimed to capture rich, raw data and contextualise participants' rationale for the convenience-privacy trade-off within their daily life experiences.

We recruited participants (see Table 2 for demographics) through an initial screening questionnaire to find people using smart home devices. We started with seven participants through social networks and expanded through snowball sampling to the remaining participants. Through this sampling, we identified participants who had experience with at least three similar smart home devices featured in the scenarios and had been using those devices for three or more months. Similar to our survey, we ensured that our interview study adhered to the ethical guidelines established by our Institutional Review Board. The majority of interviews were conducted in person (N = 10), while 6 interviews were held online via video call due to geographical constraints. Microsoft Teams was used for audio recordings, with interview durations ranging from 38 to 65 min (average: 53 min). The age range was 26 to 49 years, with a median age of 33. We had six female and 10 male participants, who covered various backgrounds in terms of occupation, country of residence, and family situation. While we recognise the potential limitations of conducting remote interviews, we also

Table 2. Demographics of interview participants (N = 16).

ID	Gender	Age	Profession	Location	Living With	Smart Home Devices
P1	Male	31	Travel Consultant	India	Mother	Voice and Video Assistants, Security Cameras, Smart TV, Smart lights
P2	Male	32	Researcher	England	Individual	Voice Assistants, Smart TV, Smart lights
P3	Male	49	Sales Director	Denmark	Wife and Son	Voice Assistants, Security Cameras, Robot vacuum, Smart Meter Home Displays, Smart TV, Smart lights
P4	Male	46	Electrical Engineer	India	Wife	Voice Assistants, Security Cameras, Smart TV, Smart lights
P5	Male	31	Sales-IT	India	Wife	Voice Assistants, Smart TV, Smart lights
P6	Male	28	Programmer	Germany	Partner	Voice Assistants, Smart TV, Smart lights, Smart Thermostat
P7	Male	34	Business Owner	Russia	Wife and Daughter	Voice Assistants, Smart TV, Baby Monitors, Robot vacuum
P8	Male	41	Software Engineer	USA	Husband	Voice Assistants, Smart TV, Baby Monitors, Robot vacuum, Smart Thermostat, Remote Video Recorder, Smart Refrigerator
P9	Male	37	IT Company Manager	Poland	Individual	Voice Assistants, Smart TV, Smart lights, Smart Window Blinds, Robot vacuum, Smart oven
P10	Female	33	Robotics Researcher	Denmark	Partner	Robot vacuum, Voice Assistant, Smart TV, Smart Meter Home Displays
P11	Female	28	HR Manager	Germany	Partner	Voice Assistants, Robot vacuum, Smart lights
P12	Female	26	Ph.D. Researcher	Denmark	Husband	Robot vacuum, Smart TV, Voice Assistant
P13	Female	27	Security Researcher	Germany	Husband	Voice Assistants, Security Cameras, Smart TV, Smart lights, Smart Meter Home Displays
P14	Male	34	Research Scientist	Germany	Partner	Voice Assistants, Smart lights
P15	Female	30	Software Developer	Denmark	Individual	Smart TV, Smart Meter Home Displays
P16	Female	42	Retired	Denmark	Husband and Daughter	Robot vacuum, Voice Assistant, Smart TV

recognise that in privacy and security studies, remote HCI research methods, such as online surveys or interviews, are well established to include underrepresented technology users (Redmiles, Kross, and Mazurek 2017). In our study, remote interviews allowed us to engage participants from underrepresented regions in HCI studies, including India and Russia.

At the beginning of each interview, we informed the participants that we would be discussing seven different scenarios that would involve smart home devices. We asked participants to choose which scenario they would like to start with, providing them with the names of all scenarios to select from. If the participant expressed a preference, we proceeded with the scenario they selected. For each selected scenario, we engaged participants in discussions about their personal experiences using similar smart home devices. If the participant had no preference, we chose a scenario that overlapped with their owned smart home devices and had the highest creepiness rating from the survey. We then discussed their personal experiences with their smart home devices in relation to that scenario. After completing the first scenario, we again asked the participant which scenario they would prefer to discuss next. If they had no preference, we chose the next scenario, following the same criteria (owned devices with the next highest creepiness rating). This process was repeated for all scenarios that matched the participant's owned devices. For participants willing to extend the interview, we discussed additional scenarios, focussing on devices they might be interested in owning in the future. In most cases, we concluded the interview after discussing scenarios that involved devices participants already owned. However, in three instances (P14, P5, P16), we explored scenarios involving smart home devices that participants were considering for future use.

3.3. Anonymization, data preparation and analysis

The interview transcription data were anonymized prior to analysis. The transcription process involved automated audio processing followed by manual verification to ensure accuracy. To protect the privacy of the participants, names were replaced with pseudonyms and all personally identifiable information was removed. According to qualitative research best practices, the original recordings were deleted after the creation of anonymized transcripts (McLellan, MacQueen, and Neidig 2003).

The interview transcripts were analysed by having all authors involved in the coding process. Our approach was collaborative and iterative, precluding the use of inter-rater reliability since code development was discussed and harmonised by coders throughout the process and by the full team on a weekly basis. The main author initially coded all transcripts using an open coding approach. The main author then discussed the codes with the full research team to harmonise interpretation. Through extensive code reviews by the full team throughout the process, we identified three initial emergent themes: privacy violations, ambiguity in data tracking and loss of user control.

We then used qualitative content analysis (Elo and Kyngäs 2008) to further develop and refine these three themes through iterative memoing, code co-occurrence analysis and clustering, and weekly team discussions. During this process, we also maintained a clear distinction between participants' actual experiences and their

reactions to scenarios. Codes related to real-life experiences were applied to actual instances described by participants, while reactions to scenarios were coded separately to capture anticipation emotions and speculative concerns. This distinction allowed us to explore both lived experiences and potential fears or discomfort with smart home technologies. The analysis of these discussions led to the identification of five key themes that encapsulate the primary privacy risks and emotional responses associated with smart home sensor surveillance. These themes, Persistent Privacy Fears, Creepy Personalization, Hidden Data Practices, Surveillance Awareness, and Bias and Manipulation Concerns, emerged from a wide range of devices and scenarios discussed during interviews. These themes are discussed in detail in the next section.

4. Findings

Throughout the interviews, participants shared personal opinions, experiences, and viewpoints about the smart home devices they currently use or have used in the past. During the discussions, participants organically introduced their own experiences with other scenarios/devices often highlighting overlapping creepy and unsettling encounters. This exploration was facilitated by our encouragement for the participants to recount their personal experiences with their own smart home devices. Although specific devices were often referenced, the five themes represent broader concerns that extend across multiple forms of smart technology. The most illustrative instances of these themes are highlighted in our findings to effectively demonstrate the depth and complexity of user's creepy experiences. An overview of these identified themes and their descriptions is provided in Table 3.

Table 3. Summary of smart home privacy concerns and their descriptions.

Smart Home Privacy Risks	Description
Persistent Privacy Fears	Ongoing anxieties about unauthorised data access and surveillance that continuously affect users' sense of security
Creepy Personalization	The unsettling experience of receiving hyper-targeted content that seems to intrude on personal privacy
Hidden Data Practices	The frustration and distrust arising from discovering that companies are secretly collecting and using personal data without clear user consent
Surveillance Awareness	The growing realisation and concern over being constantly watched or recorded by smart home devices
Bias and Manipulation Concerns	Worries about media bias and the potential for smart devices to manipulate user perceptions through covert data collection

4.1. Persistent privacy fears

Throughout the study, participants consistently expressed fears about unauthorised access and surveillance of data. A participant, alarmed by instances of major tech companies engaging in non-consensual data access, shared, '*I also heard about cases in which Google and other companies had been reviewing recordings…you are not anonymous*' (P10). This finding highlights the enduring fear individuals harbour about their privacy due to the potential for significant breaches when using digital devices.

Participants also voiced unease about the prospect of non-consensual surveillance by smart devices, such as video assistants. They emphasised the need for active control over data access to alleviate their discomfort, as one participant explained, '*Knowing that my video assistant could be watching and listening without my consent makes me uncomfortable. I'd want clear control over when it records and accesses my data*' (P6).

This doubt regarding non-consensual surveillance is further illustrated by the pervasive concern among participants, reflected in their discomfort over the potential disclosure of deeply personal information even from seemingly innocuous data. A participant articulated this sentiment, '*Your data could be anything abstract, but you never know how personal it can be. For example, it can be someone's room, and you may identify that, which can be so awkward. I am not happy about this*' (P9), which demonstrates increased awareness of the unpredictability and potential discomfort associated with the use of such data.

The need for transparency and control over data usage became evident during discussions on data-sharing practices. Participants expressed unease with concealed data sharing methods, linking the importance of transparent and well-presented data-sharing agreements to address their concerns. One participant succinctly captured this sentiment, '*If this robot vacuum came with a sticker clearly stating that it is cheaper for this amount of money and the vendor would like to use your data to send to advertisers, then I can decide whether to agree or not before making a purchase*' (P12).

Additionally, the participants highlighted significant privacy concerns regarding smart devices tracking their location using GPS data. Instances like these highlighted their discomfort stemming from potential implications of data misuse, emphasising the need for greater control over data collection practices. A participant shared her perspective, '*The idea of smart thermostats tracking your location through GPS data is quite disturbing. I value my privacy, and the thought of my thermostat knowing my whereabouts at all times raises significant privacy concerns for me*' (P15). Together, these quotes

reflect the emotional distress experienced by participants due to privacy concerns and the perceived intrusion of digital devices.

4.2. Creepy personalisation

Participants recounted instances where their devices appeared unusually attuned to their conversations and behaviours. A participant drew attention to the escalating prevalence of targeted advertisements. Despite often dismissing these occurrences as mere coincidences, he could not ignore the growing unease caused by the frequency with which these advertisements seemed to align with recent discussions. He expressed this sentiment, stating:

> *I mean, this whole targeted advertisement thing is happening more frequently now, maybe not with the argument part, but you know, we were just discussing something, and suddenly it pops up as an ad on some platform. So, you always tell yourself, 'Nah, it's just a coincidence'. Yeah, that's what I always say. I'm like, 'Nah, it's just a coincidence'* (P14).

Another participant expressed concern about the advertisements displayed on her Alexa device, particularly when discussing topics such as travel. She described feeling concerned about the possibility that her conversations with Alexa in the vicinity might influence the advertisements that were presented to her. This concern suggests that users are becoming more aware of the possible data-sharing practices between their devices and advertisers. As she put it,

> *So yeah, my first thought was that's quite realistic because we use our Alexa to play music a lot, but we don't have an Amazon subscription. Not really, but we get advertisements after two to three songs. I kind of got used to it and we just ignore the add, but it would become scary if there is some related to what we might have discussed, something I don't know. We discussed holidays and, sadly, Alexa will say Ohh, here cheap flights to Nepal or something like that* (P13).

The experience of a participant with a smart scale added to the sense of being watched. She associated the appearance of coincidental advertisements with the use of her fitness-related device, raising concerns about whether her scale was sharing personal data with advertisers. This case highlights the broader concern that even seemingly harmless devices may be involved in data-sharing practices. In her words,

> *When I stepped on my smart scale this morning, it felt like I was being watched. I mean, I've noticed these coincidental advertisements popping up lately, and it makes me wonder if my scale is sharing my data with advertisers. It's supposed to help me track my fitness goals, not expose my privacy concerns* (P14).

Participants generally described instances in which they feared that their devices predicted their preferences with unexpected accuracy. For example, one participant noted how discussions about a specific book with a friend led to seeing an ad for that book on his e-reader the following day. This level of personalisation raised feelings of discomfort and suspicion about the extent to which his devices were monitoring his conversations and activities which is similar to the ethical tensions identified in other privacy studies (Abdi et al. 2021; Lau, Zimmerman, and Schaub 2018). As he articulated, '*It's like my devices are reading my mind. I remember discussing a specific book with my friend, and the next day, I see an ad for that very book on my e-reader. It's creepy and, honestly, quite unnerving*' (P5).

In navigating the potential consequences of personalised recommendations from devices like the Google Assistants, it is challenging to pinpoint the exact emotional states expressed by participants. Nevertheless, we observed a nuanced interplay of conflicting emotions among participants. On one hand, there were indications of negative emotions, acknowledging concerns about the potential privacy implications associated with personalisation. During the same time, the participants expressed concerns about missing out on diverse information and news if they opted not to use the device, highlighting a desire for personalised content that transcends their past behaviours and preferences. This juxtaposition of emotions highlights the intricacies inherent in the trade-off between benefits and risks within the privacy calculus. A participant expressed this delicate balance, stating,

> *I appreciate the convenience of personalised recommendations through my Apple HomePod, but it worries me that I might miss out on important news and information that doesn't align with my past behaviour. There's more to the world than what I've clicked on before* (P3).

These instances show users' growing awareness of their devices' data collection for targeted advertisements. Despite valuing personalisation, users simultaneously grapple with discomfort and fear. The decision to continue using the device is not a simple binary choice; instead, it reflects the complex fear of missing unbiased information. At an abstract level, users' attitudes may paradoxically affirm privacy concerns as they persist in using devices despite advertisements closely aligned with private conversations and interests.

4.3. Hidden data practices

The participants highlighted the crucial role of transparency in the practices of smart device data, expressing a

strong desire for more openness with respect to the collection and utilisation of their data. One participant succinctly expressed this sentiment, '*It would be nice to have a lot of information. Which data are sent to whom and why?*' (P2). This call for transparency resonated across participants, with some suggesting practical solutions, such as using QR codes for easily accessible and understandable information. As articulated by another participant, '*Certainly not as a 20-page document, but more like a QR code that can be scanned, and you have all this information in an easy-to-understand way*' (P11).

Frustration with hidden conditions allowing companies to collect and use data without transparency was a common thread among participants. One participant expressed discontent, stating,

> *I don't like it when you buy a device, and you assume that you will get all the things that the devices are capable of, but everything is hidden behind conditions like 'we want to sell your data'. It's like a deliberate limitation of the device's potential, and I don't really like that* (P12).

This example highlighted a prevalent issue where end-users, expecting full access to a device's features, encounter hidden data-sharing conditions, contributing to negative emotions and reinforcing power imbalances between manufacturers and users.

Although participants acknowledged the importance of device performance, they stressed the simultaneous need for transparency in data practices. One participant aptly characterised this delicate balance, stating,

> *It's like walking a tightrope. On one hand, I want my devices to work flawlessly and enhance my life. But on the other hand, I don't want to feel like I've sold my soul to a tech giant. So, transparency becomes crucial. If they could just be upfront about what data they collect and how it's used, I'd feel a lot more comfortable* (P4).

The criteria for selecting devices were also discussed, with participants considering both quality and privacy concerns. As one participant clarified,

> *First and foremost, a device needs to demonstrate high quality, especially when comparing it to alternatives beyond Apple[brand]. It should not merely be a product void of advertisements; rather, I would be inclined to make a purchase based on the overall experience it offers* (P5).

These instances show the importance of clear and accessible information on data usage, the treatment of user concerns, and the finding of a balance between device quality and privacy.

4.4. Surveillance awareness

The participants showed a clear understanding of the need to have active control over their smart home devices and be aware of any surveillance when using them. In particular, a participant expressed relief to maintain control over their devices' camera sensors, emphasising the need to disable them when they were concerned about potential intrusions: '*If a camera is looking at me, I'd want to turn it off and be sure it's not recording*' (P16). In line with previous research (Tan, Kinnee, et al. 2022; Tan, Wong, et al. 2022), this trend aligns with the observations of previous studies on privacy. The insight reflects a common sentiment shared by participants, highlighting the proactive efforts they make to protect their privacy. This emphasis is especially notable when considering camera sensors, which are recognised for their substantial surveillance capabilities for capture comprehensive and detailed data.

Furthermore, participants acknowledged the importance of being aware of their devices' actions as a form of control, albeit in a passive capacity. They outlined between passive awareness, exemplified by indicators blinking during recording, and active control, which involves the direct ability to intervene. As one participant expressed,

> *Being aware is like some control of what data, for example, if there is a device and it is recording and it starts blinking trying to say it is recording, that is also a form of control but not active control.* (P10).

Participants also expressed a preference for implementing proactive measures independently, including modifying their behaviour in the presence of surveillance devices. One participant noted adjusting their speech volume when anticipating potential eavesdropping, stating, '*I prefer to take control so I don't have to change my behaviour. For example, I would start whispering when only I am informed*' (P6).

The widespread use of Virtual Private Networks (VPNs) has increased notably as a key aspect of surveillance awareness, offering relief from concerns about online monitoring by authorities. Participants mentioned a surge in the usage of VPNs, driven by the dual goals of convenience and anonymity: '*VPN usage has surged as people seek both convenience and anonymity*' (P7). This proactive response reflects a collective effort of users to counteract the monitoring of their online activities and locations by Internet service providers and authorities.

Participants vividly expressed the discomfort associated with the realisation that their smart home devices, particularly those equipped with audio sensors, could potentially eavesdrop during conversations. This emotional response shows the importance of maintaining control over the recording of the device. As one

participant articulated, '*Imagine you're in a conversation, and you suddenly realise your smart home device might be eavesdropping. That feeling of vulnerability and lack of control is unsettling. I'd much rather have the power to pause or stop any potential recording*' (P1). Participants expressed a preference for proactive measures, a nuanced understanding of control mechanisms, and an increasing reliance on privacy protection strategies, such as VPNs, to alleviate their negative emotions.

4.5. Bias and manipulation concerns

Participants consistently voiced concerns about bias and manipulation in the media, acknowledging its crucial role in information dissemination, but expressing concern about possible bias. A participant emphasised the need for media outlets to maintain impartiality, saying, '*I appreciate that media outlets are essential for reaching a wide audience, including those who are homebound and seeking to understand and learn about various topics. However, it's crucial that the media maintains impartiality in their reporting and analysis*' (P8). This sentiment reflects the negative emotions that participants experience when they perceive the media outlets to compromise impartiality.

Concerns expanded to biases in media consumption, with participants finding relief in built-in VPN apps during times of media restrictions due to global conflicts: '*My smart TV comes with a built-in VPN app, which has been a lifesaver during these turbulent times, given the ongoing media restrictions due to the conflict*' (P7). Participants grappled with the creepy notion of covert surveillance by smart devices in the context of their media consumption habits. Their negative emotions increased as they questioned whether their smart TVs silently monitored their viewing habits, potentially violating their privacy. As one participant candidly stated,

> *Using my smart home device to stay informed is convenient, but I'm increasingly concerned about the potential for surveillance. Take my smart TV, for instance; I appreciate the access to news, but I wonder if it's quietly monitoring my viewing habits. Although impartiality of the media is vital, ensuring the privacy and security of users should be paramount in these devices* (P2).

This sense of vulnerability and lack of control evoked strong emotional responses.

Issues related to gender stereotyping in media recommendations as also observed by Seymour et al. (2023), contributing to frustrations from perceived gender stereotypes:'*Lately, my smart home system [iPad] keeps suggesting action movies, sports events, and tech-related content, as if I'm supposed to be an adrenaline-junkie techie just because I'm a guy*' (P9). Similarly, participants experienced frustration with algorithmic product recommendations that seemed oblivious to their preferences. A participant shared their experience with a smart thermostat persistently recommending irrelevant products, fuelling their negative emotions:

> *Ever since I got that smart thermostat, it's been pushing these bizarre product recommendations on me. I mean, why would I need a snow shovel in the middle of summer? It's like the device has no clue about my preferences but wants to help in a nagging way* (P6).

The emotional responses of the participants, ranging from discomfort and frustration showing vulnerability and in some occasions aiming to relieve themselves of vulnerability, highlight the profound impact of privacy-related violations on their well-being in an increasingly digital and connected world.

5. Discussion

We developed seven scenarios to explore creepiness in smart home sensor surveillance and used these scenarios in semi-structured interviews (N = 16). The perceived creepiness of the participants varied across different aspects of smart home device usage-such as data access, personalisation, and media bias-indicating that what one person finds creepy or invasive can differ greatly from the experience of another.

5.1. Balancing privacy and creepiness in smart home devices

Our findings reveal that participants consistently expressed negative emotions when discussing both the scenarios presented and their personal experiences with smart home devices. These emotions vary between fear, frustration, and unease, depending on individuals' past encounters with privacy violations and their expectations of technology. A common theme underlying these negative feelings was the opaqueness perceived by our participants with their smart home devices similar to Thakkar et al. (2022). Although this opaqueness is not necessarily a new revelation and overlaps with other creepiness frameworks (Seberger et al. 2021, 2022; Shklovski et al. 2014) with factors such as hidden data practices, ambiguity in data tracking, lack of user control, surveillance awareness, and targeted advertisements based on recent activities. This combination of factors contributes to what is often described as perceived creepiness.

Perceived creepiness has been identified not only in the context of smart home devices but also in smartphone applications, largely due to the ambiguity in personal data management created by application developers. Although perceived creepiness appears to be a consistent outcome of opaqueness in interactions between users and their devices, it is highly subjective as also identified in other studies (Raff, Rose, and Huynh 2024; Reitinger et al. 2024; Shalawadi et al. 2024; Vitak 2020). For example, what one person perceives as creepy or invasive, another might find merely inconvenient. This subjectivity was evident in our interview discussions, such as the case of camera sensors in robot vacuums where one participant saw the camera as essential for efficient cleaning, appreciating its convenience, while another experienced increased discomfort after learning about the camera's presence.

Our interviews predominantly highlighted microphones and cameras as the most creepy, this trend aligns with previous studies (Shalawadi et al. 2024; Tan, Wong, et al. 2022; Vitak 2020) where these sensors are considered the most privacy invasive. Scenario validation also confirmed this, with video and voice assistant scenarios being rated as the creepiest. Despite these trends, we recognise that other sensors and smart home devices can also evoke high levels of perceived creepiness for some users. For example, one participant found smart scales creepy due to the ambiguity around the tracking of physiological data, while another viewed GPS tracking in smart thermostats as particularly invasive. While studies (Pierce 2019a; Shalawadi et al. 2024; Windl, Schmidt, and Feger 2023) have rightly focussed on designing intuitive methods for blocking and unblocking cameras and microphone sensors, we also recommend that designers give similar attention to other smart home sensors, considering the subjective nature of perceived creepiness. For example, a smart thermostat could provide ongoing, subtle feedback (for example, an icon when data are shared). Such continuous, low-effort interactions whilst in the background can help diverse smart home users maintain a mutual understanding of their privacy risks and in the process alleviate their perceived creepiness.

It is not surprising that users often prioritise the convenience of smart home devices over their perceived creepiness. However, our findings suggest that users still seek ways to mitigate the factors that contribute to opaqueness in their interactions with these devices. Although Do et al. (2023) introduced the concept of perceptible assurance of privacy, where users receive clear feedback on when microphones are active, this concept can be extended to other sensors and smart home devices. For example, a smart thermostat could have a physical toggle or slider that users must adjust to start collecting data, to ensure that they are fully aware when monitoring begins. Unlike always-on sensors that remain in standby mode or can be activated remotely, intentionally powered sensors require specific user actions, such as pressing a button or flipping a switch, to begin functioning. These sensors offer users direct control over activation, reducing unintentional data collection and providing visible assurance that the sensor is inactive when not in use.

Although perceptible assurance features are straightforward for certain sensors, such as cameras (Ahmad et al. 2020; Pierce 2019b; Windl, Schmidt, and Feger 2023), applying them across a range of sensors to address subjective creepiness remains challenging due to the varying privacy–convenience trade-offs that different users experience. Shalawadi et al. (2024) found that automatic physical controls on smart home sensors were perceived as particularly creepy, despite providing visible cues, because users felt they were relinquishing control to an automated mechanism. In contrast, manual controls were seen as less creepy but were often considered inconvenient by primary users, while secondary users and guests appreciated the ability to manage devices manually.

In light of these findings, we recommend that designers develop hybrid privacy solutions that combine automated and manual control options, allowing users to customise their privacy settings based on their preferences. For instance, a thermostat could present a small privacy slider on its touchscreen that lets the household choose between 'always-on automation', 'manual confirmation', or a 'hybrid mode' where the device operates automatically but pauses when new types of data are collected until the user approves. Similarly, a robot vacuum could display a short prompt in its companion app before activating its camera, giving the user the option to proceed automatically or to request explicit manual confirmation. Such design sketches illustrate how hybrid solutions can preserve convenience while still offering clear points of control. We see these as important for reducing feelings of helplessness (Shklovski et al. 2014), apathy (Hargittai and Marwick 2016), or cynicism (Lutz, Hoffmann, and Ranzini 2020), which can shape long-term privacy attitudes, especially when technology malfunctions. Moreover, they can address the diverse needs of different user groups by giving both primary and secondary users tangible ways to negotiate convenience and creepiness in everyday domestic life.

5.2. Role of consent to control perceived creepiness

Our findings suggest most participants consistently perceived hidden data practices and non-consensual data access as creepy, as this discomfort heightened their feelings of vulnerability and unease. In such cases, they desired consent as a form of control to alleviate perceived creepiness with their smart home devices. Participants emphasised the importance of active consent (Strengers et al. 2021), meaning they expected to be clearly informed and given the opportunity to approve or deny data collection as an ongoing negotiation. This expectation goes beyond initial consent agreements such as end user license agreements, as users wanted real-time, transparent control over when and how their data is being accessed, particularly with devices like video assistants or smart thermostats. For example, they expressed the need for live notifications or prompts whenever devices were recording or collecting data, allowing them to respond or adjust settings instantly. However, in many cases, the process of obtaining consent was often unclear, buried in lengthy terms and conditions, or implied through the use of the device rather than being actively sought. This undermined the participants' sense of control because they did not fully understand what they agreed to or how their data would be used. Without clear and ongoing transparent consent, participants felt they were losing control over their privacy, which contributed to their discomfort and a sense of vulnerability when interacting with smart home devices.

These concerns around consent and unclear data practices also resemble privacy discomfort in adjacent digital domains. In social media, for example, users often report unease when advertisements appear to reflect private conversations or recent searches. This discomfort is typically tied to the lack of clear explanation for how and when data was collected or shared (Nadon et al. 2018; Zhang, De Choudhury, and Grudin 2014). Similarly, in mobile apps, users have reported creepiness when permissions are requested retroactively, after data access has already occurred (Seberger et al. 2022). In these digital domains, users can often take quick actions such as closing the app, switching platforms, or adjusting settings to regain a sense of control.

In contrast, our participants found it much harder to manage creepiness in smart homes. Because these devices are embedded in shared domestic spaces and often operate continuously in the background, users described a lack of awareness about when data collection was occurring or how to stop it. This constant presence made it more difficult to withdraw or intervene, unlike in mobile or online settings. As a result, feelings of creepiness often turned into longer-term emotions normalised as showing helplessness or becoming resigned in not knowing what actions to take. This aligns with findings by Zeng and Roesner (2019), who emphasise the ambient, invisible nature of smart home surveillance. Participants described feeling misled when discovering features like built-in GPS after installation, or frustrated when muting microphones had no effect. These moments contributed to a growing sense of resignation, as users felt they lacked effective means of intervention.

In addition to concerns about sensors, our findings emphasise the role of temporality in data management. Participants found targeted advertisements particularly creepy when based on recent personal data, such as private conversations or location information. This type of advertising can be creepy and, in some regions, potentially illegal. However, our findings also revealed a paradox that despite perceiving targeted ads as creepy, participants still found them more useful than less precise ads. We believe that despite the discomfort caused by the personalised nature of these ads, participants appreciated the relevance and convenience they offered as also observed by Acquisti (2023), adding further complexity to the privacy versus convenience trade-off. This differs from the findings on online privacy (Zhang, De Choudhury, and Grudin 2014), where targeted ads were consistently perceived as creepier than less accurate targeting. As in previous studies (Geeng and Roesner 2019; Knijnenburg et al. 2022; Koshy et al. 2021; Raff, Rose, and Huynh 2024; Zimmermann et al. 2019), we found that what people consider sensitive data used for targeted advertising is subjective and our findings point to factors such as technical knowledge, past experiences with privacy violations, and the context in which the data is used.

In the previous section, we suggested that designers implement perceptible assurance through a combination of manual and automatic controls for smart home sensors, focussing on hardware solutions with clear, tangible ways to manage privacy. However, to address the perceived creepiness of targeted advertisements related to temporality in data management, we recommend designers also consider the software perspective, which contributes to discomfort through the non-consensual use of personal data for economic gain. Specifically, designers should focus on active consent (Strengers et al. 2021) by clearly informing users about the timing and source of the data used for ads, helping users feel more in control and reducing the unease associated with intrusive data practices. This

approach could help reduce users from feeling a false sense of security, believing that disabling a camera or microphone is enough to protect their privacy, while their data are still being collected and processed in the background by the software. This is especially true for targeted ads based on recent activities as also observed in the findings of mute buttons in smart home speakers by Lau, Zimmerman, and Schaub (2018).

5.3. Breaking the normalisation of perceived creepiness

In interpreting our findings, we observe that our participants tend to normalise perceived creepiness. This normalisation occurs as users gradually accept repeated privacy violations, such as being unaware of active sensors, and intrusive experiences, such as stereotypical targeted advertisements (Seymour et al. 2023). The convenience provided by smart home devices plays a crucial role in this normalisation process. As highlighted by Huberman (2021), convenience is not just a desirable consumer good but operates as an ideology that justifies and perpetuates new forms of surveillance and data extraction under the guise of enhancing the user experience. In the context of smart home devices, this ideology suggests that users may tolerate or even come to expect certain privacy invasions as a trade-off for the convenience these devices provide. Over time, the normalisation of creepiness and discomfort reflects a broader societal trend in which convenience is prioritised over privacy, leading users to accept intrusive technologies as an inevitable part of modern life.

Although this interpretation of normalising creepiness in favour of convenience is not a new revelation and was also evident in our findings. Seberger et al. (2022) also found a similar pattern: when data practices are perceived as ambiguous or unclear, users often continue to use the smartphone application despite experiencing discomfort, eventually making the discomfort to become a part of the application user experience. This paradox of normalising discomfort and thus experiencing creepiness was also observed by Acquisti (2023). Our findings too reveal a similar trend in which participants, despite recognising discomfort and privacy concerns with their smart home devices, continue to engage, and in some cases, secondary users are insisted to engage by the primary users of the smart home devices.

These findings also relate to the privacy paradox identified by Kim et al. (2023), which describes the gap between what people express about privacy and how they actually behave. Our study adds an emotional dimension to this gap in the context of smart homes. Participants were aware of privacy risks but felt that actions such as changing settings or turning off sensors were ineffective or only worked temporarily. This led to feelings of resignation or helplessness, where discomfort was not resolved but became part of everyday routines. Over time, this resulted in quiet acceptance, where creepiness did not disappear but instead became something participants tolerated. We argue that this is not a lack of concern appearing as apathetic privacy attitudes. But, the result of repeated failed attempts to manage privacy in a system that felt unchangeable.

We believe that users are aware of this paradox and have a desire to break the normalisation of perceived creepiness. We suggest that designers can support this by helping users actively challenge and overcome this acceptance of discomfort in favour of privacy. We recommend designers to use existing HCI experience frameworks, which can provide designers with a structured vocabulary for categorising and making sense of identified factors, such as users' past experiences and expectations of smart home devices. Moreover, the frameworks can enable designers to more effectively assess users' emotional responses to their interactions with smart home devices. In particular, designers can have a deeper understanding of the subjective nature of creepiness by observing how discomfort and creepiness manifest in everyday smart home use and eventually guide the creation of more user-centric and privacy-conscious designs. We suggest one such experience framework, which is 'Understanding Experience in Interactive Systems' by Forlizzi and Battarbee (2004) that emphasises three types of user-product interactions: fluent (automatic, effortless), cognitive (focused, problem-solving), and expressive (personalizing, emotional connection). It categorises experiences as experience (ongoing interaction), an experience (memorable event), and co-experience (socially shared meaning).

We believe that the three user-product interactions (Battarbee and Koskinen 2005; Forlizzi and Battarbee 2004) of fluent, cognitive, and expressive can help break the normalisation of perceived creepiness in smart home interactions. We interpret using fluent interactions as continuous, low-effort interactions whilst in the background can help diverse smart home users maintain a mutual understanding of their privacy risks and in the process alleviate their perceived creepiness. For example, a smart thermostat could provide ongoing, subtle feedback (for example, an icon when data are shared).

Wright, Shank, and Yarbrough (2022) suggest that training significantly improves user confidence, adoption, and usage of smart home technologies. Building

on this, we argue that cognitive interactions that provide clear and understandable information about data use are crucial in helping users manage their privacy. By simplifying privacy management through focussed learning moments, such as interactive tutorials, the process becomes more transparent and less daunting, reducing the creepiness associated with ambiguous data collection. Wright, Shank, and Yarbrough (2022) also highlight the importance of continuous training and support to sustain user engagement and address ongoing privacy risks. Furthermore, Solove (2021) points out how companies often create 'frictionless sharing' environments, encouraging users to share data effortlessly. When privacy protection requires effort, like adjusting settings or opting out, users are less inclined to act due to the added friction. This explains why, despite valuing privacy, users may neglect protective measures when the process feels burdensome. Designers must be aware of the negative impact of friction when incorporating privacy education into cognitive interactions, ensuring these processes remain user-friendly and empowering. We recommend that designers implement simplified privacy management systems that minimise friction while providing ongoing support. This could include interactive tutorials, real-time guidance, and clear notifications that empower users to manage their privacy without compromising convenience.

Previous smart home privacy studies (Lau, Zimmerman, and Schaub 2018; Seymour et al. 2023) have demonstrated that feelings associated with privacy risks are heavily influenced by contextual factors, such as who receives the data and what type of data is being shared. Abdi et al. (2021) found that users' acceptance of data sharing differs based on the recipient (e.g. partners vs. third-party providers) and the nature of the data (e.g. banking information vs. music playlists). Similarly, our findings reveal that secondary users, those who do not manage the device setup, often rely on the technical expertise of primary users within the household. These secondary users, who typically face higher privacy risks, may not have control over the device settings and their data sharing preferences might be overlooked. To support expressive interactions, we recommend that designers enable a collaborative setup experience for smart home devices, involving all household members. This approach would allow primary users to adapt default settings based on the privacy concerns of secondary users, ensuring that their preferences are taken into account.

We believe that the three user-product experiences (Battarbee and Koskinen 2005; Forlizzi and Battarbee 2004) of experience, an experience and co-experiences can also help break the normalisation of perceived creepiness in smart home experiences. We interpret using experience (continuous interaction) (Forlizzi and Battarbee 2004) as users gradually accept discomfort from data collection as part of daily life. By integrating these interactions, designers can reduce unsettling moments, preventing them from becoming routine in users' everyday experiences with smart homes. Our findings highlight specific creepy experiences, like the sudden appearance of targeted ads after private conversations, which can be valuable for designers. These striking moments offer clear, actionable feedback on the privacy risks users are most aware of and eager to address. By focussing on these standout instances, designers can prioritise solutions that directly mitigate prominent privacy concerns, aligning with the concept of an experience (Forlizzi and Battarbee 2004) to enhance privacy and reduce discomfort.

People are naturally inclined to share their smart home experiences, and we drew on such anecdotal evidence from forums like Mozilla's Privacy Not Included (Mozilla Foundation n.d.), where users rate the creepiness of smart home devices, to develop our interview scenarios. From our findings, we identified temporality in data management as a key issue, particularly in non-consensual targeted ads based on recent activities, which heightened discomfort. Similarly, we suggest designers actively seek and incorporate anecdotal user feedback to identify patterns of perceived creepiness in smart home devices. This approach aligns with the concept of co-experiences (Battarbee and Koskinen 2005; Forlizzi and Battarbee 2004).

6. Limitations and future work

We recognise a significant limitation in our study, as our scope of interview did not encompass all household members, restricting our insight into diverse perspectives. This echoes the limitations of previous studies that noted a similar absence of views from secondary users and children in households (Geeng and Roesner 2019). Furthermore, our secondary user participants from the households we interviewed exhibited a reluctance to share their opinions on smart home devices. By including a few participants who were secondary smart home users (P10, P11, and P16), we were able to observe some diverse views beyond primary smart home device users. Subsequent studies are essential to explore how power dynamics within households influence the concept of privacy vulnerability (McDonald and Forte 2020).

Recent work (Hasegawa, Inoue, and Akiyama 2024) shows that usable privacy and security research remains

heavily skewed toward WEIRD (Western, Educated, Industrialized, Rich, Democratic) populations, limiting the generalizability of findings across cultural contexts. Our survey reached participants from 21 nationalities across 6 regions, broadening the diversity of perspectives on privacy norms in digital technologies. In addition, our interview study included four non-WEIRD participants, which revealed nuanced ways in which privacy perceptions are shaped by local circumstances. For example, a participant from Russia emphasised continuous vigilance due to authoritarian surveillance, while in India, privacy protection was associated with financial means. Although our dataset is too small for systematic cross-cultural comparisons, these cases highlight the importance of including non-WEIRD populations in future studies. We recommend further ethnographic work to explore cultural differences in depth and to include smart home users from emerging markets and underserved populations, such as children, older adults, and people with disabilities, to ensure a more comprehensive understanding of usable privacy.

While our qualitative approach revealed how users interpret and emotionally respond to specific smart home scenarios, future work could investigate how common these responses are across larger populations. Surveys could measure users' sensitivity to psychological aspects of creepiness, such as implied malice or unpredictability, across various devices and contexts (e.g. shared spaces or household roles), and examine whether emotional responses such as resignation or frustration correlate with specific design or usage patterns (Woźniak et al. 2021). Longitudinal and diary studies could explore how discomfort stemming from perceived creepiness evolves over time, especially as users develop coping strategies or become desensitised. Experimental research could use factorial designs to systematically vary features such as interface transparency, timing of data prompts, or levels of user control. This would help isolate the effects of specific design choices identified in our findings and clarify how these factors influence and interact with users' emotional responses to perceived creepiness.

Finally, future studies could build on recent HCI research that uses provocation as a design inquiry method to help users become aware of and question their assumptions about data flows in smart home ecosystems. Provocative prototypes (also known as provotypes) (Boer and Donovan 2012) have been used both as functional artifacts (Geeng and Author 2020; Shalawadi, Echtler, and Raptis 2024) that make data surveillance visible in domestic spaces and as conceptual tools (such as scenarios) to prompt reflection. Similar to our own approach, these methods encourage users to articulate their privacy concerns and examine how those concerns align or conflict with their values. Prior work has shown that such approaches are effective in studying perceived creepiness and its normalisation, which can lead to emotional states such as apathy (Shalawadi, Echtler, and Raptis 2024), resignation (Seberger et al. 2021), or helplessness (Shklovski et al. 2014). We recommend continuing to develop and apply such strategies to foster critical reflection among users of smart home and AI-enabled devices. In addition, combining these approaches with qualitative methods such as interviews or diary studies can help capture how users interpret and respond to these experiences. Similarly, quantitative methods such as pre/post surveys or behavioural measures (e.g. using pre-validated survey scales) can further assess changes in awareness, attitudes, or intentions. Together, these mixed-method approaches can provide deeper insight into how users rationalise and justify their responses to moments of creepiness with technology in everyday domestic life.

7. Conclusion

In this paper, we explored how users experience and rationalise the feeling of creepiness in relation to smart home devices and identified the key factors that contribute the most significantly to these perceptions. Our findings indicate that users experience creepiness primarily due to unauthorised data access, invasive personalisation, and covert surveillance. These feelings are heightened by the opacity in how data is collected and used, leaving users with a persistent sense of discomfort.

We observed that while users are aware of these privacy concerns, they often rationalise their continued use of smart home devices, prioritising convenience over privacy. This paradox, where users recognise discomfort but tolerate it for the benefits of smart home technologies, is driven by the normalisation of these invasive practices. Factors such as temporality in data management, especially targeted ads based on recent activities, intensify the perceived creepiness, suggesting the need for timely transparency in data usage. To mitigate these privacy concerns, we recommended that designers adopt hybrid privacy solutions that offer both manual and automated controls, along with transparent, real-time feedback mechanisms. Finally, we suggested applying the user-product interaction framework of Battarbee and Koskinen (2005); Forlizzi and Battarbee (2004) to break the normalisation of perceived creepiness through ensuring users are both aware of and in control of how their data is managed.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Deutsche Forschungsgemeinschaft[406053132]

ORCID

Sujay Shalawadi http://orcid.org/0000-0003-3937-5427
Dimitrios Raptis http://orcid.org/0000-0001-6983-6795
Florian Echtler http://orcid.org/0000-0002-7175-9503

References

Abdi, Noura, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. "Privacy Norms for Smart Home Personal Assistants." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21)*, Article 558, 14 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411764.3445122.

Acquisti, Alessandro. 2023. "The Economics of Privacy at a Crossroads." In *Economics of Privacy*. University of Chicago Press.

Acquisti, Alessandro, and Jens Grossklags. 2005. "Privacy and Rationality in Individual Decision Making." *IEEE Security & Privacy* 3 (1): 26–33. https://doi.org/10.1109/MSP.2005.22.

Ahmad, Imtiaz, Rosta Farzan, Apu Kapadia, and Adam J. Lee. October, 2020. "Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy." *Proceedings of the ACM on Human-Computer Interaction* 4 (CSCW 2): Article 116, 28 pages. https://doi.org/10.1145/3415187.

Apthorpe, Noah, Pardis Emami-Naeini, Arunesh Mathur, Marshini Chetty, and Nick Feamster. September, 2022. "You, Me, and IoT: How Internet-Connected Consumer Devices Affect Interpersonal Relationships." *ACM Transactions on Internet of Things* 3 (4): Article 25, 29 pages–29. https://doi.org/10.1145/3539737.

Battarbee, Katja, and Ilpo Koskinen. 2005. "Co-experience: User Experience as Interaction." *CoDesign*1 (1): 5–18. https://doi.org/10.1080/15710880412331289917.

Boer, Laurens, and Jared Donovan. 2012. "Provotypes for Participatory Innovation." In *Proceedings of the Designing Interactive Systems Conference (Newcastle upon Tyne, United Kingdom) (DIS '12)*, 388–397. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2317956.2318014.

Braunstein, Alex, Laura Granka, and Jessica Staddon. 2011. "Indirect Content Privacy Surveys: Measuring Privacy without Asking about It." In *Proceedings of the Seventh Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania) (SOUPS '11)*, Article 15, 14 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2078827.2078847.

Chalhoub, George, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020. "Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study." In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI EA '20)*, 1–9. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3334480.3382850.

Do, Youngwook, Nivedita Arora, Ali Mirzazadeh, Injoo Moon, Eryue Xu, Zhihan Zhang, Gregory D. Abowd, and Sauvik Das. 2023. "Powering for Privacy: Improving User Trust in Smart Speaker Microphones with Intentional Powering and Perceptible Assurance." In *32nd USENIX Security Symposium (USENIX Security 23)*, 2473–2490. Anaheim, CA: USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/do.

Elo, Satu, and Helvi Kyngäs. 2008. "The Qualitative Content Analysis Process." *Journal of Advanced Nursing* 62 (1): 107–115. https://doi.org/10.1111/jan.2008.62.issue-1.

Enck, William, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. June, 2014. "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones." *ACM Transactions on Computer Systems* 32 (2): Article 5, 29 pages–29. https://doi.org/10.1145/2619091.

Forlizzi, Jodi, and Katja Battarbee. 2004. "Understanding Experience in Interactive Systems." In *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (Cambridge, MA, USA) (DIS '04)*, 261–268. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1013115.1013152.

Geeng, Christine, and Anonymous Author. 2020. "EGregor: An Eldritch Privacy Mental Model for Smart Assistants." In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI EA '20)*, 1–9. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3334480.3381827.

Geeng, Christine, 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 (Glasgow, Scotland Uk) (CHI '19)*, 1–13. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300498.

Guhr, Nadine, Oliver Werth, Philip Peter Hermann Blacha, and Michael H. Breitner. 2020. "Privacy Concerns in the Smart Home Context." *SN Applied Sciences* 2 (2): 1–12. https://doi.org/10.1007/s42452-020-2025-8.

Hanson, Julia, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. "Taking Data out of Context to Hyper-personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI '20)*, 1–13. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3313831.3376415.

Hargittai, Eszter, and Alice Marwick. 2016. "'What Can I Really Do?' Explaining the Privacy Paradox with Online Apathy." *International Journal of Communication* 10.

Hasegawa, Ayako A., Daisuke Inoue, and Mitsuaki Akiyama. 2024. "How WEIRD Is Usable Privacy and Security Research?." In *33rd USENIX Security Symposium*

(USENIX Security 24), 3241–3258. Philadelphia, PA: USENIX Association. https://www.usenix.org/conference/usenixsecurity24/presentation/hasegawa.

Huberman, Jenny. 2021. "Amazon Go, Surveillance Capitalism, and the Ideology of Convenience." *Economic Anthropology* 8 (2): 337–349. https://doi.org/10.1002/sea2.v8.2.

Kientz, Julie A., Shwetak N. Patel, Brian Jones, Ed Price, Elizabeth D. Mynatt, and Gregory D. Abowd. 2008. "The Georgia Tech Aware Home." In *CHI '08 Extended Abstracts on Human Factors in Computing Systems (Florence, Italy) (CHI EA '08)*, 3675–3680. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1358628.1358911.

Kim, Yeolib, Seung Hyun Kim, Robert A. Peterson, and Jeonghye Choi. 2023. "Privacy Concern and Its Consequences: A Meta-analysis." *Technological Forecasting and Social Change* 196:122789. https://doi.org/10.1016/j.techfore.2023.122789.

Knijnenburg, Bart P, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano. 2022. *Modern Socio-Technical Perspectives on Privacy*. Springer Nature.

Koshy, Vinay, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "'We Just Use What They Give Us': Understanding Passenger User Perspectives in Smart Homes." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21)*, Article 41, 14 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411764.3445598.

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

Lenhart, Anna, Sunyup Park, Michael Zimmer, and Jessica Vitak. October, 2023. "'You Shouldn't Need to Share Your Data': Perceived Privacy Risks and Mitigation Strategies among Privacy-Conscious Smart Home Power Users." *Proceedings of the ACM on Human-Computer Interaction* 7 (CSCW2): Article 247, 34 pages. https://doi.org/10.1145/3610038.

Lutz, Christoph, Christian Pieter Hoffmann, and Giulia Ranzini. 2020. "Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany." *New Media & Society* 22 (7): 1168–1187. https://doi.org/10.1177/1461444820912544.

McDonald, Nora, and Andrea Forte. 2020. "The Politics of Privacy Theories: Moving from Norms to Vulnerabilities." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI '20)*, 1–14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3313831.3376167.

McLellan, Eleanor, Kathleen M. MacQueen, and Judith L. Neidig. 2003. "Beyond the Qualitative Interview: Data Preparation and Transcription." *Field Methods* 15 (1): 63–84. https://doi.org/10.1177/1525822X02239573.

Meng-Schneider, Nicole, Rabia Yasa Kostas, Kami Vaniea, and Maria K. Wolters. 2023. "Multi-user Smart Speakers – A Narrative Review of Concerns and Problematic Interactions." In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (Hamburg, Germany) (CHI EA '23)*, Article 213, 7 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3544549.3585689.

Mozilla Foundation. n.d. "Privacy Not Included." Homepage, Whopublished = https://foundation.mozilla.org/en/privacynotincluded/, Year = 2023, Note = '[Online; Accessed 12-October-2023]'.

Nadon, Guillaume, Marcus Feilberg, Mathias Johansen, and Irina Shklovski. 2018. "In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms." In *Proceedings of the 9th International Conference on Social Media and Society (Copenhagen, Denmark) (SMSociety '18)*, 138–149. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3217804.3217906.

Ngo, Thao, and Nicole Krämer. 2022. "Exploring Folk Theories of Algorithmic News Curation for Explainable Design." *Behaviour & Information Technology* 41 (15): 3346–3359. https://doi.org/10.1080/0144929X.2021.1987522.

Oulasvirta, Antti, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. 2012. "Long-Term Effects of Ubiquitous Surveillance in the Home." In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*, 41–50. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2370216.2370224.

Park, Sunyup, Anna Lenhart, Michael Zimmer, and Jessica Vitak. 2023. "'Nobody's Happy': Design Insights from Privacy-Conscious Smart Home Power Users on Enhancing Data Transparency, Visibility, and Control." In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 543–558. Anaheim, CA: USENIX Association. https://www.usenix.org/conference/soups2023/presentation/park.

Phelan, Chanda, Cliff Lampe, and Paul Resnick. 2016. "It's Creepy, but It Doesn't Bother Me." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (San Jose, California, USA) (CHI '16)*, 5240–5251. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2858036.2858381.

Pierce, James. 2019a. "Lamps, Curtains, Robots: 3 Scenarios for the Future of the Smart Home." In *Proceedings of the 2019 on Creativity and Cognition (San Diego, CA, USA) (C&C '19)*, 423–424. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3325480.3329181.

Pierce, James. 2019b. "Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Glasgow, Scotland Uk) (CHI '19)*, 1–14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3290605.3300275.

Pierce, James, Richmond Y. Wong, and Nick Merrill. 2020. "Sensor Illumination: Exploring Design Qualities and Ethical Implications of Smart Cameras and Image/Video Analytics." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI,*

USA) (CHI '20), 1–19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3313831.3376347.

Raff, Stefan, Stefan Rose, and Tin Huynh. 2024. "Perceived Creepiness in Response to Smart Home Assistants: A Multi-method Study." *International Journal of Information Management* 74:102720. https://doi.org/10.1016/j.ijinfomgt.2023.102720.

Redmiles, Elissa M., Sean Kross, and Michelle L. Mazurek. 2017. "Where Is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics." In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (Denver, Colorado, USA) (CHI '17)*, 931–936. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3025453.3025673.

Reitinger, Nathan, Bruce Wen, Michelle Mazurek, and Blase Ur. 2024. "What Does It Mean to Be Creepy? Responses to Visualizations of Personal Browsing Activity, Online Tracking, and Targeted Ads." *Proceedings on Privacy Enhancing Technologies* 2024: 715–743.

Sadowski, Jathan. 2020. *Too Smart: How Digital Capitalism Is Extracting Data, Controlling Our Lives, and Taking over the World*. MIT Press.

Seberger, John S., Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. "Empowering Resignation: There's an App for That." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21)*, Article 552, 18 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411764.3445293.

Seberger, John S., Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. "Still Creepy after All These Years:the Normalization of Affective Discomfort in App Use." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22)*, Article 159, 19 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3491102.3502112.

Seymour, William, Xiao Zhan, Mark Coté, and Jose Such. 2023. "A Systematic Review of Ethical Concerns with Voice Assistants." In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (Montréal, QC, Canada) (AIES '23)*, 131–145. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3600211.3604679.

Shalawadi, Sujay, Florian Echtler, and Dimitrios Raptis. 2024. "Dr. Convenience Love or: How I Learned to Stop Worrying and Love My Voice Assistant." In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction (Uppsala, Sweden) (NordiCHI '24)*, Article 31, 14 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3679318.3685364.

Shalawadi, Sujay, Christopher Getschmann, Niels van Berkel, and Florian Echtler. 2024. "Manual, Hybrid, and Automatic Privacy Covers for Smart Home Cameras." In *Proceedings of the 2024 ACM Designing Interactive Systems Conference (Copenhagen, Denmark) (DIS '24)*, 3453–3470. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3643834.3661569.

Shklovski, Irina, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Toronto, Ontario, Canada) (CHI '14)*, 2347–2356. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2556288.2557421.

Shvartzshnaider, Yan, Schrasing Tong, Thomas Wies, Paula Kift, Helen Nissenbaum, Lakshminarayanan Subramanian, and Prateek Mittal. 2016. "Learning Privacy Expectations by Crowdsourcing Contextual Informational Norms." *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing* 4:209–218. https://doi.org/10.1609/hcomp.v4i1.13271.

Solove, Daniel J. 2002. "Conceptualizing Privacy." *California Law Review* 90 (4): 1087–1155. https://doi.org/10.2307/3481326.

Solove, Daniel J. 2021. "The Myth of the Privacy Paradox." *The George Washington Law Review* 89: 1–50.

Stark, Luke, and Karen Levy. 2018. "The Surveillant Consumer." *Media, Culture & Society* 40 (8): 1202–1220. https://doi.org/10.1177/0163443718781985.

Strengers, Yolande, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Florian 'Floyd' Mueller. 2021. "What Can HCI Learn from Sexual Consent? A Feminist Process of Embodied Consent for Interactions with Emerging Technologies." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21)*, Article 405, 13 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411764.3445107.

Tabassum, Madiha, Tomasz Kosinski, and Heather Richter Lipford. 2019. "'I Don't Own the Data': End User Perceptions of Smart Home Device Data Practices and Risks." In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 435–450. Santa Clara, CA: USENIX Association. https://www.usenix.org/conference/soups2019/presentation/tabassum.

Tan, Neilly H., Brian Kinnee, Dana Langseth, Sean A. Munson, and Audrey Desjardins. 2022. "Critical-Playful Speculations with Cameras in the Home." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22)*, Article 485, 22 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3491102.3502109.

Tan, Neilly H., 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 (CHI '22)*, 1–25. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3491102.3517617.

Thakkar, Parth Kirankumar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "'It Would Probably Turn into a Social Faux-Pas': Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22)*, Article 404, 13 pages.

New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3491102.3502137.

Vitak, Jessica. 2020. "Feature Creep or Just Plain Creepy? How Advances in 'Smart' Technologies Affect Attitudes toward Data Privacy." *Annals of the International Communication Association*.

Wellendorf, Kassandra, Karen Søilen, and Kristin Veel. 2022. "Calm Surveillance in the Leaky Home: Living with a Robot Vacuum Cleaner. Automating Visuality: The Image beyond Representation, Edited by Dominique Routhier, Lila Lee-Morrison, and Kathrin Maurer. Special Issue." *MAST: The Journal of Media Art Study and Theory* 3 (1): 41–62.

Westin, Alan F. 1968. "Privacy and Freedom." *Washington and Lee Law Review* 25 (1): 166.

Windl, Maximiliane, Albrecht Schmidt, and Sebastian S. Feger. 2023. "Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes." In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (Hamburg, Germany) (CHI '23)*, Article 70, 16 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3544548.3581167.

Wong, Richmond Y., Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. "Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras." In *Proceedings of the 2023 ACM Designing Interactive Systems Conference (Pittsburgh, PA, USA) (DIS '23)*, 1093–1113. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3563657.3596012.

Woźniak, Paweł W., Jakob Karolus, Florian Lang, Caroline Eckerth, Johannes Schöning, Yvonne Rogers, and Jasmin Niess. 2021. "Creepy Technology:What Is It and How Do You Measure It?." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21)*, Article 719, 13 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411764.3445299.

Wright, David, Daniel B. Shank, and Thomas Yarbrough. January, 2022. "Outcomes of Training in Smart Home Technology Adoption: A Living Laboratory Study." *Communication Design Quarterly Review* 9 (3): 14–26. https://doi.org/10.1145/3468859.3468861.

Yao, Yuan, Li Huang, Yi He, Zhijun Ma, Xuhai Xu, and Haipeng Mi. 2023. "Reviewing and Reflecting on Smart Home Research from the Human-Centered Perspective." In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (Hamburg, Germany) (CHI '23)*, Article 143, 21 pages. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3544548.3580842.

Zeng, Eric, Shrirang Mare, and Franziska Roesner. 2017. "End User Security and Privacy Concerns with Smart Homes." In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 65–80. Santa Clara, CA: USENIX Association. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng.

Zeng, Eric, and Franziska Roesner. 2019. "Understanding and Improving Security and Privacy in Multi-user Smart Homes: A Design Exploration and in-Home User Study." In *28th USENIX Security Symposium (USENIX Security 19)*, 159–176. Santa Clara, CA: USENIX Association. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng.

Zhang, Hui, Munmun De Choudhury, and Jonathan Grudin. 2014. "Creepy but Inevitable? the Evolution of Social Networking." In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (Baltimore, Maryland, USA) (CSCW '14)*, 368–378. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2531602.2531685.

Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster. November, 2018. "User Perceptions of Smart Home IoT Privacy." *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW): Article 20, 20 pages. https://doi.org/10.1145/3274469.

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

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile books.