Manual, Hybrid, and Automatic Privacy Covers for Smart Home Cameras

Sujay Shalawadi
sujaybs@cs.aau.dk
Aalborg University
Aalborg, Denmark

Christopher Getschmann
cget@cs.aau.dk
Aalborg University
Aalborg, Denmark

Niels van Berkel
nielsvanberkel@cs.aau.dk
Aalborg University
Aalborg, Denmark

Florian Echtler
floech@cs.aau.dk
Aalborg University
Aalborg, Denmark

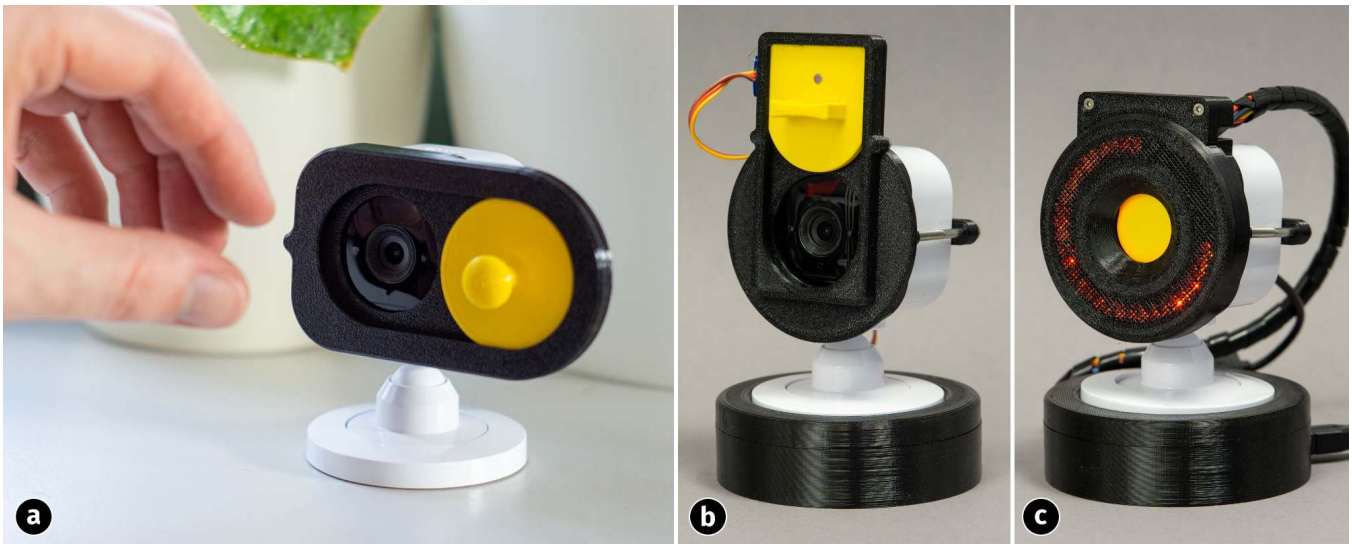


Figure 1: Three prototypes for selective camera blocking concepts of smart home cameras. a) Manual blocking: The user slides the yellow lens cap on the camera. b) Hybrid blocking: the smart home device lets a lens cover fall in front of the camera after usage. The cover needs to be raised manually. c) Automated blocking: An actuated cover slides in front of the lens or retreats. The cover is clearly visible. Before removing the cover, the lights in a ring around the lens flash.

ABSTRACT

Smart home cameras (SHCs) offer convenience and security to users, but also cause greater privacy concerns than other sensors due to constant collection and processing of sensitive data. Moreover, privacy perceptions may differ between primary users and other users at home. To address these issues, we developed three physical cover prototypes for SHCs: Manual, Hybrid, and Automatic, based on design criteria of observability, understandability, and tangibility. With 90 SHC users, we ran an online survey using video vignettes of the prototypes. We evaluated how the physical covers alleviated privacy concerns by measuring perceived creepiness and trustworthiness. Our results show that the physical covers were well received, even though primary SHC users valued always-on surveillance. We advocate for the integration of physical covers into future SHC designs, emphasizing their potential to establish a shared understanding of surveillance status. Additionally, we provide design recommendations to support this proposition.

DIS '24, July 01–05, 2024, IT University of Copenhagen, Denmark

ACM ISBN 979-8-4007-0583-0/24/07
https://doi.org/10.1145/3643834.3661569

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in ubiquitous and mobile computing**; *Interactive systems and tools.*

KEYWORDS

smart home cameras, privacy, lens cover, trust, creepiness

ACM Reference Format:
Sujay Shalawadi, Christopher Getschmann, Niels van Berkel, and Florian Echtler. 2024. Manual, Hybrid, and Automatic Privacy Covers for Smart Home Cameras. In *Designing Interactive Systems Conference (DIS '24), July 01–05, 2024, IT University of Copenhagen, Denmark.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3643834.3661569

1 INTRODUCTION

Smart home cameras (SHCs) are popular across a variety of everyday use cases and can be purchased as video doorbells, security cameras, or integrated into other smart home products such

as videoconferencing portals, vacuum robots, and pet treat dispensers. Among the many sensors integrated into smart home devices, cameras cause the greatest privacy concerns compared to other smart home sensors because SHCs are typically designed to constantly record sensitive and raw content without consent, and this could become problematic when data is abused for malicious purposes by device owners and organizations that can track user behaviour [11, 52, 56, 65, 92]. This vulnerability is further exacerbated when contemporary popular SHCs products are designed as 'always-on' devices, with no means to be sure if an SHCs is recording or to prevent it from doing so [57, 81].

Privacy concerns within smart home contexts are unevenly experienced by users and non-users of smart home devices, owing to the diverse composition of permanent and temporary household occupants, including guests. Prior research on the repercussions of continuous surveillance of such devices in multifaceted households has identified factors such as varied device requirements, different levels of technical proficiency, and different mental models of the functioning of technology, leading to disparate privacy perceptions [18, 38, 77, 85, 88]. Understanding the current state of SHCs ('*Is it recording right now?*') is essential for all people exposed to this type of surveillance. To provide inclusive privacy to people even without technical experience, sensor-level regulation has been proposed to be more reliable and safe because it is perceptually intuitive and not opaque like software solutions [56–58]. At the same time, the complete shutdown of the device can be an option to alleviate privacy concerns, although it is not preferable to the primary and frequent users of these devices [81].

In response to better understand sensor-level SHCs regulations for inclusive privacy, we developed three prototypes for camera covers: *Manual*, *Hybrid*, and *Automatic* (see fig.1). These physical covers employ tangible interaction and allow individual users to perceive and control the sensing capabilities of an SHCs, regardless of background. The concepts were built around three design criteria: *observability*, *understandability*, and *tangibility*. In our study, we focus on indoor SHCs because these devices record user footage that is rich, vivid, and deeply textured content in the most intimate physical spaces of the home, such as bedrooms [21].

We developed video vignettes of the devices and crowdsourced subjective perceptions of creepiness and trust from a sample of 90 SHCs users, a sample size larger than what is possible with longitudinal evaluation. Although our quantitative results suggest a preference for SHCs without covers, further analysis reveals that those who favor uncovered SHCs are less concerned about privacy. Qualitative findings uncover a pattern of primary users downplaying household members' privacy concerns, normalizing constant recording for home security. Simultaneously, participants employ workarounds to obstruct camera lenses. Emphasizing the fluid and contextual roles of primary and non-users, we highlight situational practices, advocating tangible solutions like physical covers. In light of these observations, we propose design recommendations for future SHC implementations. Our discussions extend the impact of physical covers beyond research by making the physical cover accessible for end users, acknowledging study limitations, and suggesting future work.

In the following sections, we provide an overview of the literature and then detail our rationale for designing physical cover prototypes and the corresponding evaluation method. Finally, we conclude by including our findings in the discussion of the applicability of physical covers to future SHCs.

2 RELATED WORK

Physical privacy covers with SHCs touches on a wide range of topics. We outline the general privacy research on smart homes, their inhabitants, and the arising tensions. To address this, a multitude of privacy-enhancing technologies have been proposed, both purely digital and physical. Relevant for evaluation is the perception of creepiness and trust as metrics on its perception by users.

2.1 Privacy Tensions and Power Dynamics in Smart Homes

Smart homes accommodate a wide range of permanent and temporary users, as well as bystanders. These people have vastly different needs [18], skill-levels [18, 38, 47, 86, 88] and privacy expectations [75], which are changing over time [54]. These secondary users may include spouses [18, 38], children [49, 75], housemates [40], visitors [48], domestic workers [40], or tenants [46]. Baumer more generally refers to this category as *usees*, "individuals who neither are clearly users of a system nor are clearly non-users" [3]. This group is reported to have incomplete mental models [18, 38, 47, 86, 88] and re-purpose mental models from non-smart devices [1]. Furthermore, the existing power dynamics in relationships is often reinforced with the introduction of smart home devices, including domestic abuse [4] and spying [7]. Another factor which reinforces these existing power dynamics lies in the design of smart home devices for a male-centric user base with stereotypically feminized digital assistants like Alexa or Siri [71]. Typically, primary users, who tend to be male, have female partners who are (claimed to be) usees or passive users of smart home devices [18, 38].

Although various kinds of data from smart home appliances are used for domestic surveillance, ranging from smart lights [7] to smart home cameras [23], the perceived impact differs greatly. Inferred data from non-audio/video devices, such as thermostats or smart lights, are underestimated [91], while both the presence and acquired data of devices with microphones and cameras are considered the most invasive [2, 54, 88]. Cameras generally cover larger areas than other sensors and can be described as "*spatially sensitive and perceptually powerful*" [23]. These cameras exist on a delicate balance between providing security for homes against various threats and creating new vulnerabilities by intruding into the most private and intimate spaces. Smart home security cameras serve as poignant examples and symbols of the challenges, compromises, and concerns arising from the integration of surveillance devices into the personal and private domains of our homes. For SHCs, in particular, their first use case as a home security device is often only the basis for their purchase before they are repurposed [21]. Using these cameras for parenting purposes (overt surveillance of minors), covert surveillance of domestic workers, or for entertainment (watching nature, pets, or family members) is common [7, 23].

2.2 Privacy-Enhancing Techniques and Sensor Level Regulations

In co-habitual spaces, the privacy tension between users and usees to actively control surveillance devices has shown that non-users show common privacy-seeking behaviors and evasion techniques. These techniques include requesting deactivation by the owner, disabling the offending device themselves by unplugging, or blocking the input by covering [1, 7, 54, 86] and jamming [8, 26, 35, 79, 84]. Although several software-based techniques have been proposed, some adversarial such as network traffic analysis [30, 50, 53] and some cooperative like blurring by request [12, 55, 63], a majority of the related work presents physical approaches. Even before smart home devices became widespread, webcam covering has been widely used and investigated as planned behavior [44, 45], describing the main motivation for using a webcam cover as an internal reassurance of security. In practice, after-market camera covers for webcams or smartphone cameras are widely available. Camera blockers integrated into commercially available products can be found on laptops (with sliding covers, swivelling mounts [31] or in retractable keycaps [42]) as well as in smart home devices (with clip-ons [33] and sliding covers [32]). All of them are manually operated, some of them can be permanently removed (clip-ons), and some serve multiple purposes (swivel-mounted laptop webcams for angle adjustment). Improving on purely manual blockers, Do et al. [14] presented variable-opacity webcam covers supporting automatic blocking based on camera state, improving perceived trust and utility by highly visible state changes.

The concepts of visibility and override informed the design of other camera probes for smart home environments. The Peekaboo Cam [9] makes use of two different privacy mechanisms to increase acceptability with participating families. The camera is unblocked automatically with a grace period and the option to abort, or camera unblocking is requested via an audio prompt. In the wearable context, Koelle et al. [36] explored the social acceptability of data glasses and found privacy violations due to pervasive recording. They suggest changing form factors and using physical blockers to signal intention of use[1]. Status LED became a common privacy notice for camera sensors, but lack of uniformity led to trust issues, with people resorting to workarounds (e.g., Post-Its on camera lens). Koelle et al. [37] further studied privacy notices beyond LED lights and discovered that LED indicators can be spoofed, undermining security. A physical mechanism, such as blocking the camera lens in webcams, can improve trustworthiness [45]. All of these approaches have in common that there is some variation of tangible interaction involved, placing an object in front, on top, or near the device to be manipulated. Ahmad et al. [1] describe this as a "stronger sense of empowerment and control" and argue that this tangible interaction is expected to perform better for usees. They would also benefit from the privacy assurances made by tangible objects [7]. However, devices independent of tangible privacy control may appeal only to a minority of usees [13].

2.3 Creepiness and Trust

The term creepiness has been widely used in pervasive technologies that are perceived as threatening privacy [83]. For SHCs in particular, Pierce et al. illustrate the notion of creepiness as critical in addressing privacy research [3, 56, 58]. Cameras are seen as a potential source of sharing, stealing, or misusing digital information, posing risks to the privacy and well-being of those to whom the data belong. Similarly, in other privacy contexts where tracked data is commodified, creepiness was associated with the feeling of being followed [76, 92]. Another perspective of Shklovski et al. [69] found that creepiness was related to situations where people became accidentally aware of data flows from technology that violate their privacy and often lead to learned helplessness. In summary, creepy user experiences in technology use can arise from first impressions and aesthetics [83], violation of expectations [69], and perceived social unacceptability [75].

In privacy research within and beyond HCI, trust functions as a counterweight to vulnerability and loss of power in the disclosure of personal data [78]. According to Moyano et al.[51], trust is "*the personal, unique and temporal expectation that a trustor places on a trustee regarding the outcome of an interaction between them*". In our case, the trustor, the SHCs user, requires the trustee (physical cover) to perform an action. Trust is fundamental to helping the trustor decide which trustee to consider in order to initiate the interaction and accept its outcome (avoiding surveillance). In other fields, trust is closely related to security in Information Technology [17] and in the Internet-of-Things [27]. While manufacturers explicitly emphasize the convenience aspect of SHCs, the implications for privacy are not always clearly communicated. In the era of surveillance capitalism [92], devices and appliances transcend being mere commodities; they serve as data production tools. Understanding trust dynamics becomes essential as users often face trade-offs between perceived conveniences of SHCs and the potentially hidden privacy implications in this evolving technological landscape [57, 81].

3 PHYSICAL CAMERA COVERS: PROTOTYPE DESIGN

Privacy concerns in smart homes often arise spontaneously, such as incidents involving accidental exposure (e.g., being inadvertently seen by a camera), or chronically, stemming from the persistent surveillance of always-on cameras [54, 56]. To effectively address these concerns, any approach to enhancing the privacy of SHCs must consider both types of problems.

Additionally, issues exist with prerequisites for interacting with smart home devices. Some users may lack interest in or understanding of digital devices, access to a smartphone, awareness of vendor-specific apps, or knowledge of device-specific credentials. In such cases, usees may need to rely on a primary user for assistance. This social issue can be mitigated by implementing default behaviors that minimize the need for social negotiations, or by facilitating equal access through tangible interaction. An example found in many smart voice assistants is the use of physical mute buttons. However, as reported by Lau et al. [40], these buttons are challenging to comprehend, less trustworthy, and infrequently utilized.

Alternative approaches proposed for SHCs, such as content-based blurring, may be more challenging for usees to understand and verify. Leveraging other modalities, such as ambient lighting or audio cues, can enhance usees' perception of control [57]. Based

[1] https://www.thingiverse.com/thing:96237

on the literature and the identified issues, we derive three main criteria for sensor blocking in SHCs that can benefit both users and usees in smart homes:

(1) **Observability.** Essential for trust and acceptance is the ability to observe the current recording state of a device, ideally from any point within the range of the camera. If the device is equipped with a camera blocker, one should be able to observe the mechanism, confirming its proper operation. From afar, the blocker should aid in observing the device's state (blocked or unblocked). This is in line with the privacy recommendations of Langheinrich [39] for notifying about data collection. A similar concept has been used successfully in Peekaboo [9], a camera probe for ethnographic research that combines a camera blocker with a speaker and a red flag to ensure observability.
(2) **Understandability.** While understanding the full capabilities and state of a smart home device may not be possible or necessary, the state of its sensors should be understandable at a glance. Similarly to how unplugged devices are universally understood to be *off*, this also applies to physical covers. A visible physical cover over a lens indicates that the device is in a 'safe' state, whether it is on, off, or on standby. If this physical mechanism is sufficiently simple, it can be understood by observation, as long as it does not challenge existing mental models. A good understandability effect can be seen with variable-opacity films on the smart webcam cover [14] and head-mounted eye wear devices [70].
(3) **Tangibility.** A person within the range of the camera sensor should be able to interact with the device, asserting control to abort or prevent unauthorized recording. Interactions that require a smartphone with a device-specific app, an account, and access rights raise the barrier to assert control. On a spectrum of interactions to maintain control, direct tangible manipulation can be the one with the lowest barrier. This is synonymous with other ad-hoc evasion techniques, such as covering or unplugging. The tangible interaction provides direct feedback, making the act of blocking more observable and understandable as well.

However, there is a limitation when combining tangible interaction with understandability and observability, a spatially close connection of the device, mechanism, and outcome is required. Although a home may contain many smart home devices, adhering to all three concepts makes a cover necessarily specific for a single device. Consequently, a person may have to interact individually with multiple SHCs in the same space, as any generalizable approach to control many devices simultaneously would be inherently more abstract and less understandable (see [13]). In conclusion, potential SHCs camera covers should be: 1) as simple as possible within reason; 2) making use of physical mechanisms as revealing the 'gears and cogs' may help to decrease the leap of faith needed by people to trust the system; 3) have a visible default state, helping in reducing social friction and making it easier to induce preferred behavior.

3.1 Prototype Development

We developed three types of lens covers as attachments to a popular smart home camera, the Amazon Blink Mini[2]. The Blink Mini is a common type of SHCs: an indoor security camera that can easily be repurposed for many tasks. It has no hardware buttons and can solely be controlled by a paired app on a smartphone. The only information directly provided is the recording activity indicated by a blue light on the front. Building physical prototypes for an existing SHCs allows us to rely on participants' familiarity with the base concept, and enables us to gauge the impact of benefits and drawbacks more accurately than with a purely conceptual study, both internally during the building process and externally with the participants through the survey [64].

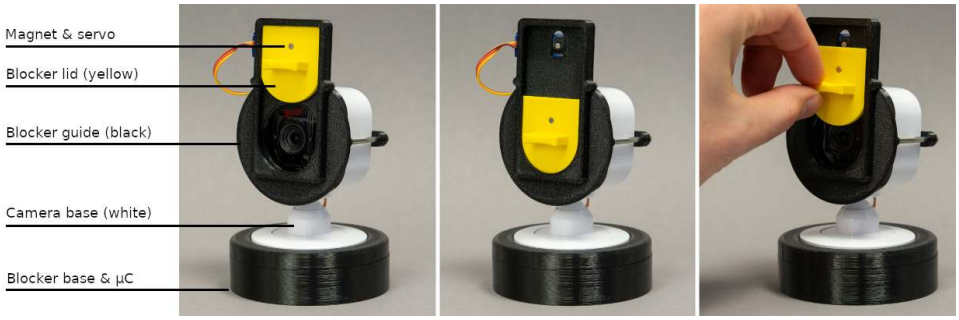
The three prototypes offer different levels of convenience and automation around trust and control issues related to the camera sensor:

- The manual cover (see Fig. 2a) is a slider that can be attached to the camera. It is bright and easy to recognize across the room (see Fig. 3). This type of sensor cover is the most simplistic design and does not enforce a default state. The sensor is blocked or unblocked, depending on the last manual interaction; the cover does not change state by itself.
- The hybrid cover (see Fig. 2b) behaves similarly to the manual cover but re-engages without manual intervention after recording stops. The cap is held magnetically. Once the camera stops recording, a servo moves the magnet for a moment and allows the cap to drop. Before the SHCs can record again, the cap must be manually lifted. This is a blocked-by-default configuration, requiring manual interaction before usage.
- The automatic cover (see Fig. 2c) moves the cap itself and requires no manual intervention; the sensor is blocked by default. Once the camera is about to initiate a recording, a countdown is shown around the lens as a ring of lights to resemble a clock face. When the countdown ends, a servo retracts the cap, uncovering the sensor. If a physical button on the device is pressed, the cover will remain closed or close again if already opened. Thus, this is an unblocked-by-default configuration that allows the device to work unobstructed if no action has been taken. The state of the device cover, and thus the recording ability of the device, is always visible.

We designed three fully functional add-ons to investigate trust and control issues commonly found in widely used SHCs like the Amazon Blink Mini. Similar to previous studies [37, 58], we found that people often struggle to trust that the camera is off and may forget when the camera is on, leading to privacy concerns. Although manual and automatic covers may seem to be clear options that sit at the opposite spectrum for ease of use, we also focused on hybrid covers to specifically tackle the problem of people forgetting about the presence of a camera. We chose a bright, hi-viz color for the blocking lid to create contrast with the camera's enclosure. The automatic and hybrid cover detects camera activity by measuring the power consumption of the device, providing a straightforward and less invasive solution compared to analyzing network traffic.

[2]https://www.amazon.com/Blink-Mini-White-1Cam/dp/B07X6C9RMF

(a) Manual Camera Cover



(b) Hybrid Camera Cover

(c) Automatic Camera Cover

Figure 2: The three cover prototypes as add-ons to a Blink Mini smart home camera. The manual cover (a) requires to manually move the cap. The hybrid cover (b) lets the cap slide down automatically, but requires the user to manually lift it before next usage. The automatic cover (c) makes use of a motorized cap that opens and closes automatically but displays a countdown using the LED ring (red: counting down, blue: recording), allowing to abort manually through a button press before opening.

The source code and CAD files for the 3D-printed prototypes are available at OSF.

The three prototypes offer different levels of privacy measures compared to the unmodified smart home camera. The automatic cover requires minimal effort, as it changes state automatically based on camera activity, benefiting primary users, while still allowing usees to object to being recorded by pressing the integrated abort button during the pre-recording countdown. The hybrid cover requires explicit unblocking, preventing detection without prior interaction from both groups of users. The manual cover requires direct interaction for every state change, the most straightforward but least convenient option. These trade-offs were evaluated in a user study, detailed in the following section.

4 METHOD

Our objective was to understand how the participants perceive SHCs in general and how physical covers affect perceived creepiness and trust. To avoid inflated responses about privacy concerns [6, 69], we used video vignettes of smart home camera covers without explicitly mentioning privacy issues. Vignettes allowed us to systematically present different hardware modifications and have been used for studying privacy concerns in various contexts (see, e.g., [25, 28, 43]). We created one vignette for each physical shutter prototype and an additional one without any physical shutter. Each video lasted 30-40 seconds and was filmed in a home environment for relatability. We conducted two surveys, a methodology which

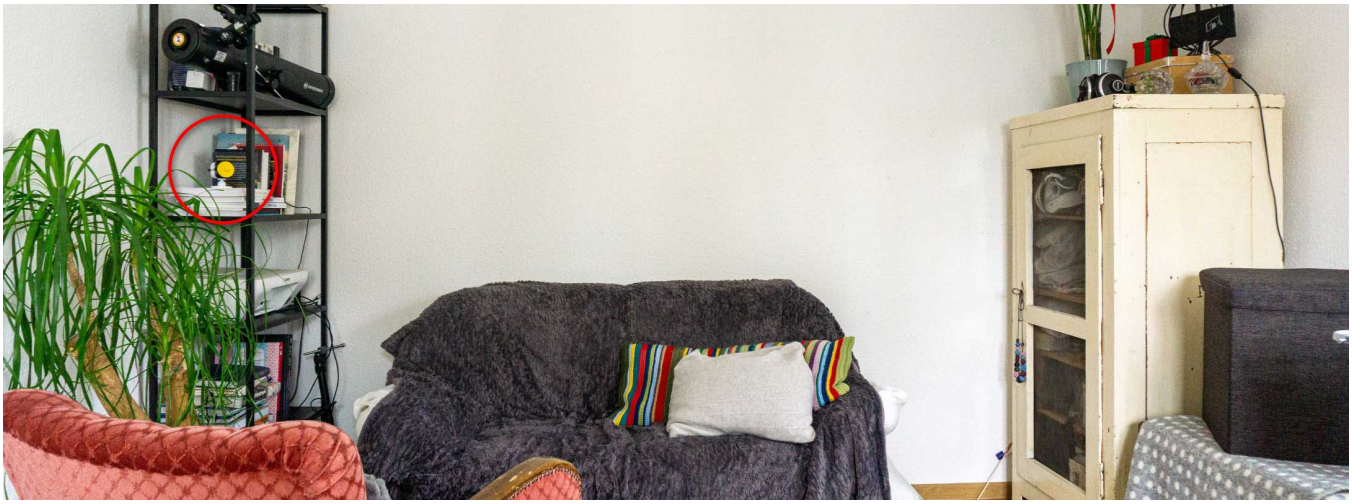


Figure 3: A physical cover as an extension for a commercial SHCs is designed to be noticeable at arbitrary locations within a living space.

has previously been used to better understand smart home privacy perceptions (see e.g., [73, 87]). The two surveys are described below.

4.1 Survey 1: Identifying participants

In survey 1, our objective was to identify potential participants by verifying ownership of an indoor SHCs. We presented example images of indoor SHCs to confirm participants' self-reported usage. Additionally, we collected demographic information (age, self-identified gender, coarse geographic location, household size) and explored the context of SHCs usage, including acquisition, setup, and placement decisions. Privacy perceptions were evaluated using the Smart Home Privacy Concern Scale by Guhr et al. [19], focusing on four subscales: (1) secondary use of information (SUoIP), (2) perceived surveillance (PS), (3) perceived intrusion (PI), and (4) awareness of privacy practices (AoPP), which are relevant to the concerns addressed by physical covers. SUoIP evaluates the extent to which individuals are concerned about the potential misuse of data collected by smart home devices. PS measures users' feelings of being monitored or watched by their smart home devices. PS focuses on the extent to which individuals feel that smart home technologies intrude on their personal life and space. AoPP measures the degree of awareness that individuals have regarding the privacy practices associated with their smart home devices. The privacy concern scale, previously employed in studies on smart devices among older adults [59], trust in chatbots in the insurance industry [60], or user-centric privacy controls for smart homes [10], includes an attention check question, and the order of the questions was randomized. Open-ended responses about the purpose of the SHCs were coded for significant themes by two authors. Participants who failed the attention check were excluded from subsequent analysis.

4.2 Survey 2: Vignette evaluation

Participants meeting the criteria in survey 1 progressed to survey 2, viewing four vignettes in a Latin Square randomized order. Each vignette was followed by 20 Likert scale questions, including 8 from the Perceived Creepiness of Technology Scale (PCTS, see Appendix B.1) [83] and 12 from the Human Computer Trust Scale (HCTS, see Appendix B.2) [20], encompassing all subscales. PCTS, designed to measure technology-related "creepiness", derives from privacy studies associating the term with potentially privacy-threatening technologies. The three dimensions of PCTS — implied malice, undesirability, and unpredictability — capture perceived creepiness in our SHCs vignettes in relation with privacy measures that our prototypes can offer.

HCTS, validated for consistency within design fiction scenarios simulating intimacy, particularly in smart home contexts [66], features five subscales focusing on technological system ethics and morality. HCTS assesses trust and expected consequences in user interactions with the technological system. The final section comprised free-text responses (see Appendix B), prompting participants to rank the vignettes, express preferences, and provide insights into their understanding. Likert-scale questions were randomized, and an attention check ensured response quality. The free text responses were subjected to a deductive thematic analysis [5]. There were a total of 410 free-text responses from 82 participants who volunteered to provide their opinions. We used Atlas.ti (https://atlasti.com/) for data analysis and proceeded as follows. Initially, the main author selected the most informative responses, leading to the formation of 39 preliminary codes. We then honed in on specific codes that provided deeper insights into our quantitative findings. For example, the "family dynamics" was one of the codes we considered to be valuable. It explored how users of SHCs balanced the convenience of continuous surveillance with the potential impacts on household privacy due to the camera's shutter options. This examination was part of a broader discussion that evolved through four rounds of collaborative discussions with all authors, culminating in the thematic coding of the data into four distinct themes which are presented in the qualitative findings. The details of the codes can be found in Section 7.

4.3 Participants and Procedure

Participants were recruited through Prolific Academic. To ensure sufficient response quality, we restricted participation to crowdworkers with an acceptance rate of 95% or higher. We conducted two iterations with the same participants. We offered the UK minimum wage of £10.42 per hour at the time of the study as suggested by Prolific, i.e. £1.60 for survey 1 with an expected completion time of 9 minutes and £3.50 for survey 2 with an expected completion time of 20 minutes (both durations based on our pilot studies).

To minimize type 2 errors, we define the number of participants based on a power calculation using G*power [16]. Given the exploratory nature of our investigation, we used small to medium effect sizes (f^2 = 0.15), an alpha level of 0.05, and a power of 0.8, according to established methodological recommendations [24]. Based on these parameters, the minimum required sample size is 62 participants. To be conservative (foreseeing dropouts) and maintain reliability, we ended up recruiting 100 participants for survey 1, of which 90 were included in the final analysis of survey 2 after excluding those who failed one or more attention check questions. The surveys were distributed to a gender-balanced sample (50% men and women).

For both surveys, participants received clear instructions emphasizing that their involvement was entirely voluntary, and they could choose not to participate if they preferred. They were also informed that they could withdraw from the surveys at any time without any consequences. We assured participants of the confidentiality of their responses, noting that the surveys would not contain any personally identifiable information. Additionally, for any inquiries or concerns, we provided an email address through which they could contact us. Although local regulations did not mandate a formal ethics review, we adhered strictly to the ethical guidelines recommended by our institution.

5 RESULTS

The participants had an average age of 37.7 years (SD = 10.2), ranging from 19 to 79. The age group breakdown of the participants is as follows: youth (18-24 years) = 6, young adults (25-34 years) = 30, middle-aged adults (35-44 years) = 35, senior adults (45-54 years) = 12, and elderly (55 years and above) = 7. participants An overview of participant demographics is provided in Table 1. Our sample spans 21 countries, with South Africa (27), United Kingdom (21), and Poland (11) being the three largest subgroups. For survey 2, ten participants incorrectly answered at least one attention check, indicating low effort or potential automation. These participants were excluded from analysis, resulting in a total of 90 participants. With this sample size, our post hoc power stands at 0.933 for small to medium effect sizes (f^2 = 0.15), considering an alpha level of 0.05 and a recommended power of 0.8 [24].

5.1 Participant Overview

Among our participants, only five respondents had no children, while the majority (N = 85) had at least one child in their household. A substantial subset (N = 23) also lived with older individuals. Most participants (N = 53) use SHCs daily, and another significant group (N = 27) uses their SHCs weekly, while 10 reported rarely using their SHCs. Overall, participants use their SHCs primarily for home

Table 1: Overview of participant demographics (N = 90).

Attribute	N	% sample
Gender		
Women	45	50%
Men	45	50%
Location		
Africa	27	30%
Europe	58	64%
North America	5	5%
South America	1	1%
# of SHCs		
Exactly 1	49	54%
More than 1	51	46%
Household Size		
Alone	1	1%
With Partner	17	18%
With Family (partner and kids)	31	34 %
With Family (partner, parents and kids)	33	36 %
Joint Family or more or more	18	19 %
Educational Level		
High School (discontinued)	1	1.1%
High School	8	8.8%
Bachelor's Degree	49	54.5%
Master's Degree	28	31.2%
PhD or Higher	4	4.4%

security, as explained by one participant, "*Monitoring doorways, passages, and the gate for intruders and movement around the yard*" (P65, Male). This was done to ensure the safety of other household members, as expressed by another participant, "*I've started using it [SHCs] because my parents take care of my children, they are now not in good shape, and I wanted to make sure that everything is fine*" (P77, Female). Furthermore, participants repurposed SHCs surveillance over time, as indicated by a response, "*Multiple uses over the years. We bought it as a baby monitor, although it wasn't designed for that. Then we used it for security, looking at the door, and now I installed it in my mother's house because she is old and I want to take a look just in case something happens (which could also double as security if I point it in the right direction and change some settings)*" (P18, Female).

More than half of our sample (N = 49) had used their SHCs for over a year, with only nine participants having recently started (less than a month). Approximately equal numbers of participants (N = 46) used more than one SHCs, while (N = 44) relied on just one. Among our participants (N = 23), some felt the need to cover the SHCs lens for comfort, and 14 explicitly mentioned intimate situations as their primary reason, citing instances like "*all the times I got out of the shower and ran for a snack naked when I am home alone*" (P27, Female) and "*intimate moments with my partner*" (P81, Male).

Regarding SHCs surveillance, our sample explicitly supported premeditated surveillance (N = 25) with a specific goal like home security, while nine participants mentioned casual surveillance

with an unplanned goal, such as looking at past footage out of curiosity. These two types of SHCs surveillance, referred to as formal and casual surveillance by Tan et al. [23], encompass a broad spectrum of everyday surveillance defined by premeditation, focus, and regularity. Most participants (N = 40) mentioned using SHCs for both types of surveillance, while ten did not mention using SHCs for surveillance, and six preferred not to disclose whether they used SHCs for surveillance. The majority of our participants (N = 75) placed their SHCs in living areas or common spaces like hallways, while a substantial subset (N = 45) placed their SHCs in more private spaces such as bedrooms and children's rooms.

In our sample, a significant proportion of SHCs users (N =67) could broadly be classified as primary users based on the introduction, self-education, and decision making related to SHCs at home. These classification criteria align with existing studies on smart homes in HCI [18, 23, 38, 88]. Specifically, the majority of users (N =56) dominated the introduction and self-education aspects of SHCs use. However, when determining the SHCs's location, a substantial number of participants (N= 53) collaborated with other household members in the decision-making process.

Participants expressed moderate privacy concerns related to SHCs, with an average score of 37.72 (SD = 8.24) out of a maximum of 55. Cumulative scores from four pertinent subscales [secondary use of information (SUoIP), perceived surveillance (PS), perceived intrusion (PI), and awareness of privacy practices (AoPP)] were considered. Figure 4 displays box plots that illustrate the distribution of normalized percentage scores on these subscales. Each box denotes the inter-quartile range (IQR) divided by the median, while Tukey-style whiskers extend to a maximum of 1.5 x IQR beyond the box. Participants, on average, demonstrated greater awareness of privacy practices with the least variability as can be seen in the figure 4.

5.2 Quantitative Analysis

We begin by evaluating participants' perceived creepiness and trust scores across the four SHCs vignettes. Following this, we explore the correlation between creepiness and trust. Given prior research indicating gender-based variations in privacy protection [34] and the predominantly male representation among primary users in smart home studies [18, 71], we extend our analysis to assess the impact of gender on participants' perceptions of creepiness and trust in the context of the four SHCs vignettes.

5.2.1 Perceived Creepiness. We calculated the perceived creepiness scores by following the PCTS protocol [83]. Table 2 summarizes the descriptive statistics per vignette. A Kolmogorov-Smirnov normality test on perceived creepiness scores showed a normal distribution for all vignettes except for the vignette with no cover with $p = 0.008$. Therefore, we conducted a Friedman test which showed that the vignettes are indeed significantly different, $\chi^2(3) = 35.07$, $p = <.001$, $\eta_2 = .12$. The distribution of the overall creepiness scores for the four vignettes can be seen in Figure 5a. Pairwise post-hoc tests using Wilcoxon signed rank tests showed that the "no cover" SHCs is perceived as significantly less creepy than any of the other SHCs. Furthermore, the participants found that the hybrid cover SHCs is significantly more creepy than the manual cover SHCs (see Table 3).

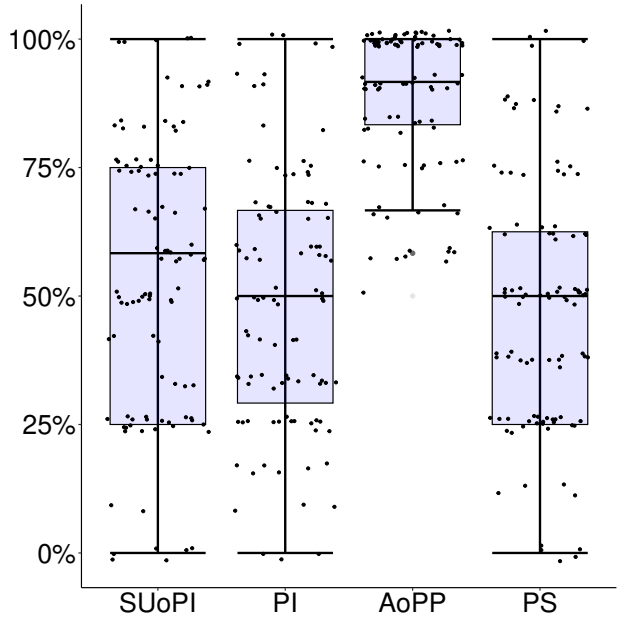


Figure 4: Box-Plot distribution for (N = 90) across the subscales from Guhr et al. [19]. The abbreviations of subscales are as follows: secondary use of information (SUoIP), perceived surveillance (PS), perceived intrusion (PI), and awareness of privacy practices (AoPP)

. The dots represent the density distribution of participants' average scores.

While these results may seem counter-intuitive at first, we discuss potential reasons in our analysis of qualitative results below.

Table 2: Descriptive statistics on perceived creepiness.

Vignette	*N*	Mean	Median	Std. dev
No Cover	90	13.07	12	4.41
Manual Cover	90	15.94	14.5	6.34
Hybrid Cover	90	18.09	17	6.54
Automatic Cover	90	16.26	16	6.62

Table 3: Pairwise post-hoc comparisons of the creepiness concerns of evaluated SHCs vignettes. P-values of Wilcoxon signed rank tests with Bonferroni corrections.

Vignettes	No Cover	Manual Cover	Hybrid Cover	Automatic Cover
No Cover	-			
Manual Cover	.007	-		
Hybrid Cover	<.001	.022	-	
Automatic Cover	.009	1.	.017	-

5.2.2 Perceived Trust. We calculated trust scores using the HCTS protocol [20], with descriptive statistics in Table 4. A Kolmogorov-Smirnov normality test confirmed a normal distribution (Figure 5b). A one-way ANOVA revealed a significant difference in mean trust scores between at least two vignettes (F(3, 270) = [19], p = <0.001, η^2 = .09). Post hoc tests (Tukey HSD) indicated that no cover had a significantly higher trust score than all other vignettes. Additionally, manual cover was more trustworthy than both hybrid cover and automatic cover. No significant differences were found between hybrid cover and automatic cover (Table 5), but significant differences were observed between no cover and hybrid cover, and no cover and automatic cover.

Table 4: Descriptive Statistics of the trust scores.

Vignette	Mean	Std.Dev	Min.	Max.
No Cover	46.58	7.44	33	60
Manual Cover	43.58	8.58	19	60
Hybrid Cover	41.18	9.37	14	60
Automatic Cover	39.81	8.48	13	55

Table 5: The p-values for the pairwise post-hoc comparisons of the trust concerns about different vignettes using Tukey HSD tests with Bonferroni corrections.

Trust	Mean diff.	Std. Error	p	95% CI
No Cover-Manual	3.02	1.072	.036	[0.89, 5.15]
No Cover-Hybrid	5.4	1.131	<.001	[3.15, 7.65]
No Cover-Automatic	6.77	0.961	<.001	[4.86, 8.68]
Manual-Hybrid	2.38	0.13	<.001	[2.12, 2.64]
Manual-Automatic	3.74	0.935	.001	[1.89, 5.60]
Hybrid-Automatic	1.37	0.965	.961	[-0.55, 3.28]

5.2.3 Correlating Creepiness and Trust. We added individual vignette scores of creepiness and trust for each participant. The mean values of creepiness and trust across the four vignettes were found to be normally distributed using the Kolmogorov-Smirnov normality test with p = .63 and p = .766 respectively. A Pearson correlation test showed that there was a significant association between creepiness and trust scores, r(88) = -0.74, p = <.001. Figure 6 shows the high negative correlation trend between the two variables, i.e. low trust corresponds to high creepiness.

5.2.4 Ranking the SHCs Vignettes. Participants ranked the four SHCs vignettes according to perceptions and fit in their homes, visualized through stacked bar plots (see Figure 7). The specific questions that prompted free-text responses can be seen in the Appendix B.3. Using *PlackettLuce* R package [74], we calculated coefficient scores for each type of SHCs. Despite a tie for the preferred choice between SHCs without cover and automatic cover, as seen in the rank 1 choice in the bar plots, nuanced insights emerged. On average, participants assigned the lowest weight (0.1910950) to the SHCs without a cover, slightly favoring manual covers (0.2294640). Hybrid covers (0.2615229) had a higher preference than manual covers and without covers, while cameras with automatic covers received the highest average preference (0.3179181). The trend of privacy concerns for the first choice of participants revealed lower concerns for those selecting no cover (M = 35.94, SD = 7.78), slightly higher for manual covers (M = 38.44, SD = 8.10), and similar concerns for hybrid covers (M = 38.67, SD = 9.62). Participants ranking cameras with automatic covers reported the highest average privacy concerns (M = 39.73, SD = 8.35). Cameras without covers were the least preferred on average, but users who chose them had the lowest reported privacy concerns. Cameras with manual and hybrid covers fell in between, and users reported moderate privacy concerns.

5.2.5 Gender. We divided our sample by self-reported gender into men (N = 45) and women (N = 45) groups. Analyzing overall privacy concerns based on Guhr et al. [19], we found that men (M = 40.57, SD = 7.44) had lower privacy concerns than women (M = 41.94, SD = 6.82). A two-tailed t-test (t(96) = -0.95, p = .345, 95% CI [-4.23, 1.49], Cohen's d = 0.19) indicated a nonsignificant difference with a small effect size. Privacy concerns distribution is shown in Figure 8a. Examining mean creepiness and trust scores across genders for all vignettes, both groups differed significantly in perceived creepiness for the manual cover. The Kolmogorov-Smirnov test showed non-normal distribution for the men's group (p = 0.043). Men (Mdn = 13) perceived lower creepiness than women (Mdn = 17) for manual cover. A Mann-Whitney U test (U = 718.5, p = .018, r = 0.25) confirmed significant differences. Descriptive statistics for sub-scales are in Table 6. The first sub-scale, implied malice, was not normally distributed. A Mann-Whitney U test showed a significant difference for the sub-scale unpredictability (t(73.26) = -3.43, p = .001, 95% CI [-2.53, -0.67]).

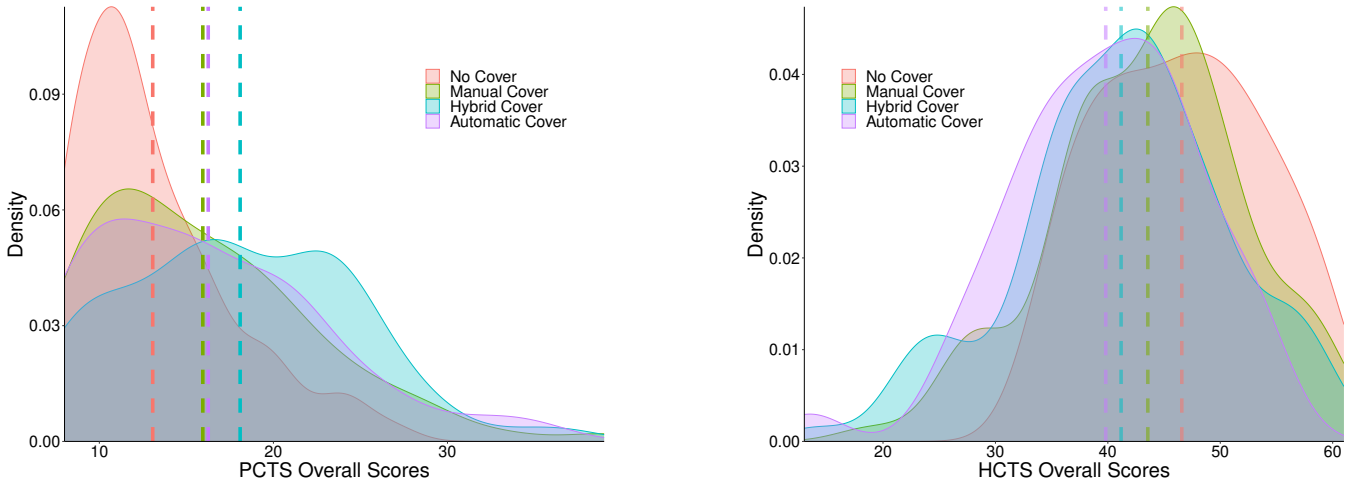
Table 6: Sub-scale Scores and Significance Tests for creepiness scale for SHCs with manual cover.

Sub-Scale	Men; Women	Var. & Sig.
Implied Malice	*Mdn*=2; 3	<0.001; U=814, p=.11, r=0.18
Undesirability	M(SD)=6.04(2.63); 7.33(3.46)	0.038; 0.05
Unpredictability	M(SD)=5.02(1.64); 6.62(2.67)	0.002; 0.001

5.3 Qualitative Analysis

To delve further into our intriguing findings, we present the four themes that resulted from our deductive thematic analysis of 410 free text responses from survey 2, provided by 82 participants who shared insights on vignette ranking motivations, their interpretation of camera sensor status, preferred physical covers, and alignment of vignettes with their privacy values. The specific questions for prompting responses from the participants can be found in the Appendix B.3.

5.3.1 ***Always-On Alert.*** Participants emphasized the importance of the always-on surveillance feature in SHCs, as one participant amusingly pointed out, "*I do not understand the logic of having a security camera that does not perform its function/can be switched off on an ad hoc basis. If one wants security, then being able to turn*



(a) Perceived creepiness scores.

(b) Perceived trust scores.

Figure 5: Distribution of creepiness and trust scores across the four SHCs vignettes. Vertical dashed lines indicate the mean values for each SHCs vignette.

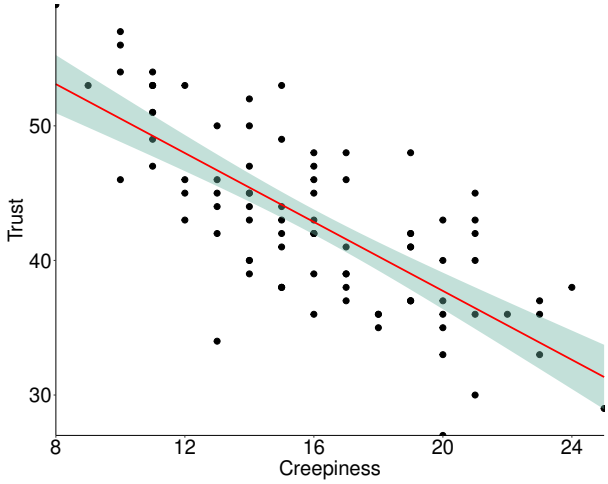


Figure 6: Correlation Significance Trend between Mean Creepiness and Trust Scores across all four Vignettes.

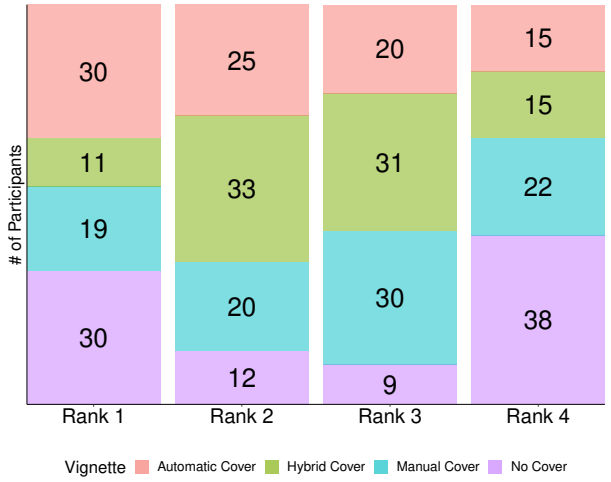
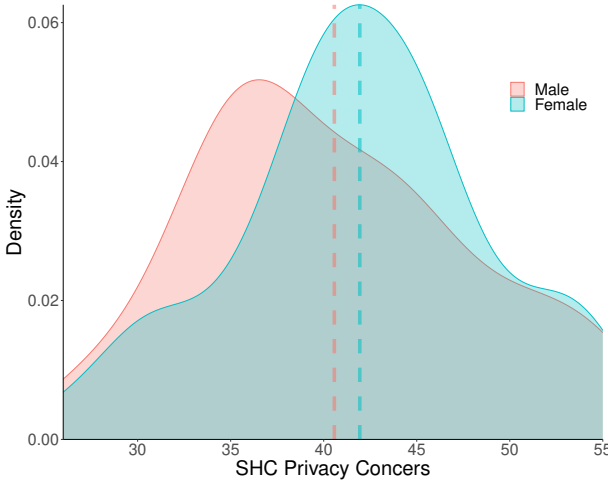


Figure 7: Preferred Choices of Vignettes when asked to rank.

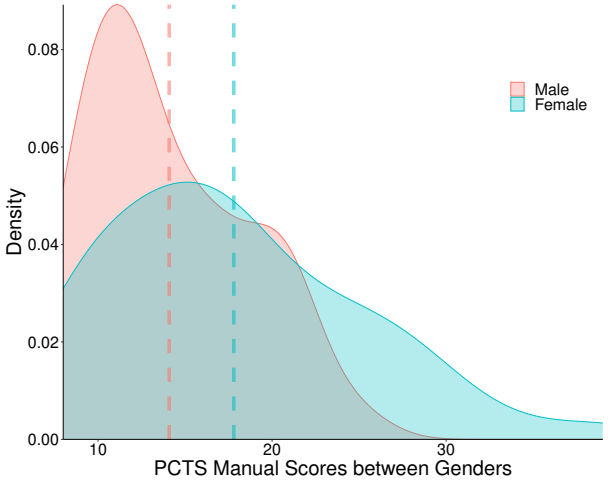
off the camera negates the usefulness of the camera. What happens if one forgets to turn off the cover and there is a security issue? Does that come down to user error or manufacturer error? The only camera that was truly suitable for purpose was the always-on mini camera" (P35, Male).

Concerns were also raised about physical covers potentially interfering with SHCs surveillance. A participant expressed, "*I picked the one with no cover because I feel like I might miss important/useful footage with the camera covered. I know that with the hybrid or manual versions, I would constantly forget to uncover the camera. The automatic one might be okay for me, but I would worry that it would miss important filming during the countdown period*" (P14, Female).

Most participants (N = 71) self-reported being the primary users of SHCs, influencing purchase decisions, installation, and location choices. The remaining 19 participants were not directly involved in setting up the SHCs or in the purchasing decisions, but they self-reported having some input on the placement of the SHCs within their homes. Primary users shaped the use of SHCs for other household members through normalization of surveillance by downplaying the privacy concerns of seniors and children. One participant nonchalantly stated, "*None of my family or friends has ever been concerned about our smart camera. And if they were, I would just reassure them that they all carry smartphones around with cameras on them all day long, how are the two any different?*" (P55, Male).



(a) Overall privacy concern scores between the men's and women's group.



(b) Overall creepiness scores between the men's and women's group for SHCs with manual cover.

Figure 8: The vertical lines represent the mean values of both groups.

5.3.2 ***Constant Surveillance is the New Normal.*** Participants highlighted the profound influence of constant surveillance on their interactions with household members, particularly children or pets. A participant humorously noted, "*I can use my voice over the camera to calm my dog, and in turn, I am reassured when I know that he is not howling and annoying the neighbors. I also have proof if they ever try to report me to the authorities*" (P43, Female).

While remote surveillance was considered crucial, physical covers were seen to empower privacy without sacrificing the benefits of remote monitoring. A participant expressed, "*I would want a camera that I can control entirely remotely, so I chose my first option [automatic cover] as the one I can remotely open or close the lens. For children, it can still be very comforting because you can speak with them to calm them if necessary. It gives them a more safe feeling*" (P3, Male).

Participants also shared their coping strategies to protect privacy, such as turning off their SHCs or rotating the camera lens away while at home. One participant revealed, "*Currently I put a book in front of my camera when I don't want it to see anything, so I'd like one of these cameras with a built-in cover*" (P5, Female). Another participant emphasized personal responsibility, stating, "*If you really want to be absolutely certain, if you are that scared for privacy, don't put the camera in a position to invade your privacy in ways you don't want*" (P51, Male). The normalization of surveillance extended to guests, with one participant asserting, "*I don't consider others' feelings in my home or guests. If someone feels invaded by my smart home camera, they can leave or not visit. Life is about choices.*" (P33, Female).

5.3.3 ***Perceptions, Concerns, Preferences and Hesitations for Physical Covers.*** The trust of the participants in an existing SHCs vendor over physical cover add-ons reflected their perceptions of showing awareness to data practises. One participant expressed, "*The uncovered camera looks the best, but it has the least protection. Yet, since it's from Amazon, a trusted company, I feel safer. The manual cover is okay, and it's guaranteed to be covered when needed. But the hybrid and automatic covers could be hacked or overridden.*" (P16, Male).

Regarding physical covers, the automatic cover raised suspicion, and was perceived as being out of control. A participant mentioned, "*The automatic cover is 4th place since it could uncover itself without me noticing, while I believe it is covered, possibly showing sensitive [information] about my life.*" (P61, Male). For manual and hybrid covers, doubts related to human errors in interacting with SHCs covers were evident. A participant commented, "*They both [manual and hybrid] just look so unsafe because you need human interaction for it to fully function.*" (P29, Female). Another participant expressed a similar concern, "*I prefer the no cover, human error comes in the mix with the others [manual and hybrid]. Timers, physical buttons and also the automatic gives kind of a false pretense of privacy security*" (P52, Male).

If users had faced highly creepy situations, then the chances of using physical covers are higher; however, they might still weigh the trade-off between privacy and security. A participant articulated, "*It's a trade-off. You might have to feel a bit creepy for getting security. I have mixed feelings. Cameras make me feel censored in some rooms but more comfortable in others*" (P27, Female).

5.3.4 ***Perceived Benefits of using Physical Covers.*** Physical covers were perceived as privacy-empowering, with one participant stating, "*I prefer using a smart home camera with lens protection. It is essential in today's world where companies often misuse personal information*" (P49, Male). Participants unfamiliar with physical covers emphasized the importance of control when they were unaware of the ongoing surveillance around them. This sense of control was summarized with a participant saying, "*I gave the manual cover the top rank because it provides me with complete control over my privacy. This sense of control is what makes me feel the most safe and secure*" (P9, Female).

Physical covers positively affected self-confidence in being aware of the recording status of SHCs. A participant mentioned, "*I believe*

their [physical covers] use norms look pretty easy. You don't have to keep track of a lot of things. But maybe that ease of use is what generates a bit of confidence: is the camera really off?" (P23, Female).

The tangible interaction and control were considered desirable, as illustrated by one participant's statement: "*I dislike the uncovered camera as it may compromise my security, giving me a feeling that it might record without my knowledge. I prefer the hybrid one because I can manually open it, ensuring it is secure*" (P38, Male). Similar sentiments were shared about the manual cover, "*With manual, everything is clear, since you control the process of closing or opening the lens, others will not be so easy to control*" (P12, Female). Primary SHCs users recognized the potential of physical covers for individuals less familiar with technology, referred to as usees. A participant expressed, "*Manual cover is easy to understand for less technical people. Adding a physical cover can make uncovered cameras less uncomfortable for guests,*" (P47, Male).

6 DISCUSSION

This section provides design recommendations for physical SHCs covers, reevaluating our initial criteria. We dive into the seemingly paradoxical behavior on why our moderately privacy concerned participants showed higher trust and lower creepiness for SHCs without physical covers. Exploring the broader implications of physical covers beyond research and academia, we acknowledge the limitations of our study and propose future directions.

6.1 Revisiting the Design Criteria: Lessons Learned

When evaluating manual and automated camera controls, participants had reservations about adding physical covers. Two key factors driving these reservations were mental load and trust, as revealed in our qualitative findings. Although manual cover appeared to be the simplest concept, it garnered higher trust scores compared to hybrid and automatic covers. However, the subjective mental load associated with remembering to interact with manual cover, coupled with perceived physical effort, was deemed high, leading to a reluctance to incorporate it into daily use. Although the manual cover appears to positively meet all three design criteria, it did not convince the participants about potential long-term use. Hybrid and automatic covers were seen to be less trustworthy and somewhat creepy, but the participants found them less mentally taxing. However, the low trust of the participants in them was directly affected by their reluctance to surrender control to another autonomous entity for the preservation of privacy.

Although a significant portion of primary users (N = 31) preferred SHCs without covers, it should be noted that most initial purchases were also SHCs without covers, as indicated by self-reported models and responses in free text. We believe that this influenced the reluctance to adopt physical covers after becoming accustomed to continuous surveillance over time. These findings may also relate to the observation that primary users who often purchase and set up SHCs themselves, are more likely to feel "in control" of these devices. As a result, they may be more concerned on whether the physical shutters impact the functionality than on privacy. With an average household size of three and SHCs often placed in shared spaces, the home transcends individual use, evolving into a space of intimate communal interaction. Despite this, primary users frequently minimize privacy concerns from other household members, accepting the pervasive nature of constant recording by existing SHCs.

To counteract the normalization of indoor surveillance, we recommend offering a choice between all three types of physical covers for future SHCs. Acceptance of these covers is influenced by factors such as mental load and trust. Although quantitative results may suggest lower preference for hybrid covers in terms of creepiness and trust, our recommendation for them values a person's confidence in knowing the camera's status (on and off) whether it may be through automatic lens blocking and the ability to manually unblock the camera based on the subjective perceptions of mental load and trust they place in the physical shutters. Our intention of also including hybrid covers could prevent users from forgetting or not knowing that the camera sensor is on, as identified in other SHCs studies [3, 22, 23].

Physical cover prototypes formalize typical privacy preservation practices, such as using sticky tapes or placing books, by integrating interactive sensor-level regulation, enhancing their visibility and usability. Recognizing that digital data are prone to leakage [29, 56, 69], SHCs as a source of raw sensor data pose a security vulnerability that must be addressed amid their increasing integration into daily life.

Physical covers for SHCs provide sensor-level regulation, unlike many smart cameras and IoT devices that rely solely on software-based LED lights [61]. We believe that these covers can serve as intuitive privacy indicators for various users, offering situational awareness to usees by their distinct appearance from the camera case (see Figure 3). Additionally, they act as justification mechanisms for usees to gauge the primary user's intentions. Moreover, these covers justify the device's status without relying on written language, color codes, or complex icons, making them accessible and user-friendly for privacy actions. These interpretations are also supported by findings from other field studies related to privacy in the smart home [1, 13, 37, 57].

Incorporating physical covers as a built-in feature aligns with the goal of making privacy protection inherent in the product's design. While providing physical covers post-hoc by separate manufacturers may seem more trustworthy to users uncertain about vendors, our findings indicate that participants generally trusted their SHCs vendors, possibly leading them to downplay privacy concerns. In addition to recommending future SHCs models include options for all three types of physical covers, we also suggest vendors integrate them as an inherent part of the product. This approach can formalize workaround blocking techniques, such as using books or tape, as identified in our qualitative findings. Our participants expressed interest in purchasing future SHCs with built-in physical covers, which is consistent with users willing to pay an additional 10% to 30% for improved privacy and security in smart home devices [15]. We estimate that all three types of covers would be financially feasible to implement within this price range.

6.2 Unpacking the Trade-off: Accounting for Fluidity and beyond Rationality

In our sample, moderately privacy conscious participants traded off privacy control from physical covers in favor of constant surveillance for home security and monitoring other household members. Our findings align with pragmatic attitudes observed in other privacy studies in which users rationalize between convenience and privacy risks [18, 38, 67, 69, 89, 90].

Furthermore, our findings highlight an affective dimension where participants felt anxious about potential privacy violations due to the misuse of the SHCs' constant audio and video surveillance capabilities. Although not a new revelation, this affective dimension emphasizes the need to look beyond pragmatism to the trade-off between privacy and convenience in various contemporary digital technologies [68]. We emphasize the importance of this affective perception, particularly in how SHCs can disproportionately benefit the economics of vendors or manufacturers over users [11, 92].

In privacy research, people often express a negative affect with the data practices of digital technologies, labeling them as creepy [68]. Our findings align with this sentiment, as creepiness arises when individual expectations clash with the capabilities of SHCs [67, 83]. Participants who prefer SHCs without covers often leverage features like remote monitoring and cloud storage, enhancing home security, but potentially compromising privacy for others. Although "surveillance as care" may be beneficial in some situations, privacy researchers caution that it can reinforce problematic power dynamics and obscure less intrusive forms of care [56, 82]. This discrepancy highlights the tension between the stated values and the actual actions.

It is crucial to remember that human actions are not purely rational but are influenced by context and circumstances. In today's data-driven economy [92], the convenience often comes at the expense of privacy, turning privacy into an idealized value that is challenging to practically achieve. This perception may appear less contradictory when different privacy preferences are considered, such as expecting primary users of SHCs to empathize with the perspective of usees.

Although the majority of our participant sample identifies as primary users, aligning with characteristics from previous studies [18, 38, 82], we observe that the distinction between primary users and usees is not strictly discrete. The primary user category is fluid and dynamic, echoing the interpretations of Wong et al. [82]. A user may be primary in one context and become a usee in another, highlighting the flexible nature of these roles.

Control remains a central theme for participants seeking ways to safeguard their privacy, employing methods such as repositioning the camera lens or choosing less intrusive locations. When distinctions between primary users and usees are blurred, physical covers for SHCs could offer users a reassuring mechanism to avoid false positives (recording without indication) and automatically respond to privacy-sensitive situations predictably and reliably.

6.3 Broader Impact

Our work extends beyond the academic HCI community by providing openly available hardware and software designs (see reproduction note) for physical blockers. These resources can benefit future studies or be directly utilized by privacy-conscious individuals. Our findings emphasize the importance, reiterated here, for designers of SHCs and related products to integrate tangible control mechanisms into their devices, offering users and particularly usees the option for greater freedom of choice.

Furthermore, we discovered that primary users often attempt to consider the perspective of their household's usees, although not through direct consultation. Our insights reveal that primary users are unsure how to reassure usees, often resorting to downplaying surveillance as a coping mechanism. To address this, we believe making our prototypes open source for tech-savvy primary users might encourage them to use these tools alongside their SHCs. This might serve as an ad-hoc solution to support reassuring usees within their household without the need for repeated explicit discussions with the primary user.

6.4 Limitations and Future Work

Our analysis comes from a crowd-sourcing platform that collected self-reported opinions from SHC users, with the majority of the sample identified as primary users based on home purchase, installation, and usage characteristics [18, 38]. Although our aim was to include participants from diverse geographical regions, our current sample lacks coverage of Oceania and Asia, the latter partly due to limited indoor SHCs use [72]. Both North and South America are underrepresented as well. Conversely, 30% of our sample (N = 27) is from South Africa, where prioritizing continuous surveillance for home security over privacy concerns may be influenced by increased experiences of assaults and home invasions in the region [62]. Likewise, participants' privacy perceptions in different geographical regions might be shaped by local factors that were not addressed in our study.To promote inclusive privacy research, we suggest incorporating emerging markets for smart home cameras from underrepresented regions [41, 80].

Considering the varied impact of indoor SHCs on household members, especially older adults and children, our findings mainly reflect the opinions of primary users (N = 71) living with secondary users/usees (N = 19) [3]. As mentioned above, this may have biased the responses towards functionality over privacy. Acknowledging these limitations of our study, we propose explicitly including the opinions of non-primary household members, guests, and other *usees* in future studies.

While our camera blockers provide visible reassurance that no video recording is taking place, they cannot provide the same level of privacy protection for audio recordings. Although the blockers do cover the camera's microphone as well, they cannot entirely prevent audio from being recorded. For future work, we recommend to explicitly look into users' perceptions about audio recording devices vis-a-vis sensor blocking mechanisms as well.

In our quantitative findings, we observed that women tend to have more privacy concerns than men. This reflects the dominance of men in the primary user group, influencing smart home device manufacturers towards a male-centric user base [18, 38, 71]. Although our primary focus was not gender specific, we observed significant gender differences in perceived creepiness with respect

to manual covers. Although beyond the scope of this paper, we recommend future studies to explore gender-specific privacy concerns related to SHCs.

Finally, our study is limited by the fact that participants could not interact directly with our prototypes, but rather viewed them as video vignettes. Our tangible prototypes in particular may lose some of their self-explanatory nature in a video. However, we consider this an acceptable limitation, as it is a widely used methodology [25, 28, 43] which enables us to reach a larger sample size than what is usually feasible with laboratory-based studies.

7 CONCLUSION

In this study, we examined user perceptions of physical covers for regulating privacy in SHCs. We developed three prototypes — manual, hybrid, and automatic — for a popular SHC model and created video vignettes demonstrating their privacy-preserving capabilities. Our investigation involved recruiting 90 SHC users to assess perceived creepiness and trust associated with these covers. Surprisingly, our quantitative analysis revealed a prevailing preference among participants for SHCs *without* physical covers. This preference stemmed from users valuing the convenience of monitoring household members and enhancing home security over privacy concerns. Notably, individuals favoring uncovered SHCs exhibited lower levels of privacy concerns compared to those advocating for physical covers. By integrating our quantitative findings with qualitative insights, we advocate for the integration of physical covers into future SHC designs, emphasizing considerations of mental load and trust. We also suggest - in line with other studies [57, 82] - that privacy is highly contextual and that physical covers can offer a common language of justification on the status of surveillance. We conclude by discussing the broader impact of the physical covers, making the prototypes publicly available, acknowledging limitations to our study, and suggesting future directions.

REPRODUCTION NOTE

The design files for the prototypes, survey data, and scripts for generating all referenced plots are available publicly:

https://osf.io/5ckmh/?view_only=4569bbbaa4574f3bad6541ee4c2cc70f.

ACKNOWLEDGMENTS

This work was supported by the German Research Foundation (DFG) through grant EC437/1-1.

REFERENCES

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (Oct. 2020), 28 pages. https://doi.org/10.1145/3415187

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (July 2018), 59:1–59:23. https://doi.org/10.1145/3214262

[3] Eric P.S. Baumer. 2015. Usees. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 3295–3298. https://doi.org/10.1145/2702123.2702147

[4] Nellie Bowles. 2018. Website. Retrieved May 12, 2023 from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[5] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.

[6] Alex Braunstein, 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)*. Association for Computing Machinery, New York, NY, USA, Article 15, 14 pages. https://doi.org/10.1145/2078827.2078847

[7] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[8] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376304

[9] Yu-Ting Cheng, Mathias Funk, Wenn-Chieh Tsai, and Lin-Lin Chen. 2019. Peekaboo Cam: Designing an Observational Camera for Home Ecologies Concerning Privacy. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. Association for Computing Machinery, New York, NY, USA, 823–836. https://doi.org/10.1145/3322276.3323699

[10] Chola Chhetri and Vivian Genaro Motti. 2022. User-Centric Privacy Controls for Smart Homes. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 349 (nov 2022), 36 pages. https://doi.org/10.1145/3555769

[11] Kate Crawford. 2021. *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

[12] Adrian Dabrowski, Edgar R. Weippl, and Isao Echizen. 2013. Framework Based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing. In *2013 IEEE International Conference on Systems, Man, and Cybernetics*. 455–461. https://doi.org/10.1109/SMC.2013.83 ISSN: 1062-922X.

[13] Sarah Delgado Rodriguez, Sarah Prange, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3546155.3546640

[14] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D. Abowd, and Sauvik Das. 2022. Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (Dec. 2022), 154:1–154:21. https://doi.org/10.1145/3494983

[15] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. *Exploring How Privacy and Security Factor into IoT Device Purchase Behavior*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[16] Franz Faul, Edgar Erdfelder, Axel Buchner, and Albert-Georg Lang. 2009. Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods* 41, 4 (2009), 1149–1160.

[17] Davide Ferraris, Carmen Fernandez-Gago, and Javier Lopez. 2018. A trust-by-design framework for the internet of things. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 1–4.

[18] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[19] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H Breitner. 2020. Privacy concerns in the smart home context. *SN Applied Sciences* 2 (2020), 1–12.

[20] Siddharth Gulati, Sonia Sousa, and David Lamas. 2019. Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology* 38, 10 (2019), 1004–1015. https://doi.org/10.1080/0144929X.2019.1656779

[21] Neilly H. Tan, 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)*. Association for Computing Machinery, New York, NY, USA, Article 485, 22 pages. https://doi.org/10.1145/3491102.3502109

[22] Neilly H. Tan, 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)*. Association for Computing Machinery, New York, NY, USA, Article 485, 22 pages. https://doi.org/10.1145/3491102.3502109

[23] Neilly H. Tan, Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. 2022. Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–25. https://doi.org/10.1145/

3491102.3517617
[24] Joseph F Hair. 2009. Multivariate data analysis. (2009).
[25] David Harborth and Sebastian Pape. 2021. Investigating privacy concerns related to mobile augmented reality Apps–A vignette based online experiment. *Computers in Human Behavior* 122 (2021), 106833.
[26] Adam Harvey. 2010. CV dazzle. Website. Retrieved May 12, 2023 from https://cvdazzle.com/.
[27] Lance J. Hoffman, Kim Lawson-Jenkins, and Jeremy Blum. 2006. Trust beyond Security: An Expanded Trust Model. *Commun. ACM* 49, 7 (jul 2006), 94–101. https://doi.org/10.1145/1139922.1139924
[28] Christine Horne and Wojtek Przepiorka. 2021. Technology use and norm change in online privacy: Experimental evidence from vignette studies. *Information, Communication & Society* 24, 9 (2021), 1212–1228.
[29] Tung-Hui Hu. 2015. *A Prehistory of the Cloud.* MIT press.
[30] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 2, Article 46 (jun 2020), 21 pages. https://doi.org/10.1145/3397333
[31] Acer Inc. 2011. Acer Orbicam. Website. Retrieved May 12, 2023 from https://www.acerrepairblog.us/aspire-3640-travelmate-2440/acer-orbicam.html.
[32] Amazon.com Inc. 2021. Amazon Echo Show 5 (2nd generation. Website. Retrieved May 12, 2023 from https://www.amazon.com/All-new-Echo-Adjustable-Stand-Charcoal/dp/B09155JR3K.
[33] Facebook Inc. 2022. Facebook Portal. Website. Retrieved May 12, 2023 from https://store.facebook.com/de/portal/.
[34] Esther D.T. Jaspers and Erika Pearson. 2022. Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research* 142 (2022), 255–265. https://doi.org/10.1016/j.jbusres.2021.12.043
[35] Bjørn Karmann. 2018. Project Alias. Website. Retrieved May 12, 2023 from https://bjoernkarmann.dk/project_alias.
[36] Marion Koelle, Matthias Kranz, and Andreas Möller. 2015. Don't Look at Me That Way! Understanding User Attitudes Towards Data Glasses Usage. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Copenhagen, Denmark) *(MobileHCI '15)*. Association for Computing Machinery, New York, NY, USA, 362–372. https://doi.org/10.1145/2785830.2785842
[37] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '18)*. Association for Computing Machinery, New York, NY, USA, 177–187. https://doi.org/10.1145/3173225.3173234
[38] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 41, 14 pages. https://doi.org/10.1145/3411764.3445598
[39] Marc Langheinrich. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing (Lecture Notes in Computer Science)*, Gregory D. Abowd, Barry Brumitt, and Steven Shafer (Eds.). Springer, Berlin, Heidelberg, 273–291. https://doi.org/10.1007/3-540-45427-6_23
[40] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 102:1–102:31. https://doi.org/10.1145/3274371
[41] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. 2021. How WEIRD is CHI?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 143, 14 pages. https://doi.org/10.1145/3411764.3445488
[42] Huawei Technologies Co. Ltd. 2021. Huawei Matebook X Pro. Website. Retrieved May 12, 2023 from https://consumer.huawei.com/en/laptops/matebook-x-pro-2021/.
[43] Christoph Lutz and Aurelia Tamò-Larrieux. 2021. Do privacy concerns about social robots affect use intentions? Evidence from an experimental vignette study. *Frontiers in Robotics and AI* 8 (2021), 627958.
[44] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam Covering as Planned Behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173754
[45] Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior. In *Proceedings 1st European Workshop on Usable Security*. Internet Society, Darmstadt, Germany. https://doi.org/10.14722/eurousec.2016.23014
[46] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* (2020). https://petsymposium.org/popets/2020/popets-2020-0035.php
[47] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM 2020)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464
[48] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020. "I don't know how to protect myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3419249.3420164
[49] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735
[50] Richard Mitev, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. 2020. LeakyPick: IoT Audio Spy Detector. In *Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. Association for Computing Machinery, New York, NY, USA, 694–705. https://doi.org/10.1145/3427228.3427277
[51] Francisco Moyano, Carmen Fernandez-Gago, and Javier Lopez. 2012. A conceptual framework for trust models. In *Trust, Privacy and Security in Digital Business: 9th International Conference, TrustBus 2012, Vienna, Austria, September 3-7, 2012. Proceedings 9*. Springer, 93–104.
[52] Johannes Obermaier and Martin Hutle. 2016. Analyzing the Security and Privacy of Cloud-Based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (Xi'an, China) *(IoTPTS '16)*. Association for Computing Machinery, New York, NY, USA, 22–28. https://doi.org/10.1145/2899007.2899008
[53] TJ OConnor, Reham Mohamed, Markus Miettinen, William Enck, Bradley Reaves, and Ahmad-Reza Sadeghi. 2019. HomeSnitch: Behavior Transparency and Control for Smart Home IoT Devices. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 128–138. https://doi.org/10.1145/3317549.3323409
[54] Antti Oulasvirta, 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)*. Association for Computing Machinery, New York, NY, USA, 41–50. https://doi.org/10.1145/2370216.2370224
[55] Frank Pallas, Max-Robert Ulbricht, Lorena Jaume-Palasí, and Ulrike Höppner. 2014. Offlinetags: a novel privacy approach to online photo sharing. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA '14)*. Association for Computing Machinery, New York, NY, USA, 2179–2184. https://doi.org/10.1145/2559206.2581195
[56] James Pierce. 2019. 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)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300275
[57] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In *Designing Interactive Systems Conference* (Virtual Event, Australia) *(DIS '22)*. Association for Computing Machinery, New York, NY, USA, 26–40. https://doi.org/10.1145/3532106.3535195
[58] James Pierce, 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)*. Association for Computing Machinery, New York, NY, USA, 1–19. https://doi.org/10.1145/3313831.3376347
[59] Pireh Pirzada, Adriana Wilde, Gayle Helane Doherty, and David Harris-Birtill. 2022. Ethics and acceptance of smart homes for older adults. *Informatics for Health and Social Care* 47, 1 (2022), 10–37. https://doi.org/10.1080/17538157.2021.1923500 arXiv:https://doi.org/10.1080/17538157.2021.1923500 PMID: 34240661.
[60] Davinia Rodríguez Cardona, Antje Janssen, Nadine Guhr, Michael H Breitner, and Julian Milde. 2021. A matter of trust? Examination of chatbot usage in insurance business. (2021).
[61] Asreen Rostami, Minna Vigren, Shahid Raza, and Barry Brown. 2022. Being Hacked: Understanding Victims' Experiences of IoT Hacking. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 613–631. https://www.usenix.org/conference/soups2022/presentation/rostami
[62] Sohel Sayyad, Arbaj Momin, Matin Shaikh, Riddhi Mirajkar, and Priya Shelke. 2023. Smart Home Surveillance System Using Artificial Intelligence. In *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)*.

1–7. https://doi.org/10.1109/ESCI56872.2023.10100088
[63] Jeremy Schiff, Marci Meingast, Deirdre K. Mulligan, Shankar Sastry, and Ken Goldberg. 2009. Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns. In *Protecting Privacy in Video Surveillance*, Andrew Senior (Ed.). Springer, London, 65–89. https://doi.org/10.1007/978-1-84882-301-3_5
[64] Albrecht Schmidt. 2017. Understanding and researching through making: a plea for functional prototypes. *Interactions* 24, 3 (April 2017), 78–81. https://doi.org/10.1145/3058498
[65] Britta Schulte, Sujay Shalawadi, Max Van Kleek, and Florian Echtler. 2021. Cloudless Skies? Decentralizing Mobile Interaction. In *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '20)*. Association for Computing Machinery, New York, NY, USA, Article 48, 3 pages. https://doi.org/10.1145/3406324.3424598
[66] Britta F. Schulte, Paul Marshall, and Anna L. Cox. 2016. Homes For Life: A Design Fiction Probe. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction* (Gothenburg, Sweden) *(NordiCHI '16)*. Association for Computing Machinery, New York, NY, USA, Article 80, 10 pages. https://doi.org/10.1145/2971485.2993925
[67] John S. Seberger, 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)*. Association for Computing Machinery, New York, NY, USA, Article 552, 18 pages. https://doi.org/10.1145/3411764.3445293
[68] John S. Seberger, 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)*. Association for Computing Machinery, New York, NY, USA, Article 159, 19 pages. https://doi.org/10.1145/3491102.3502112
[69] Irina Shklovski, 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)*. Association for Computing Machinery, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421
[70] Julian Steil, Marion Koelle, Wilko Heuten, Susanne Boll, and Andreas Bulling. 2019. PrivacEye: privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications* (Denver, Colorado) *(ETRA '19)*. Association for Computing Machinery, New York, NY, USA, Article 26, 10 pages. https://doi.org/10.1145/3314111.3319913
[71] Yolande Strengers and Jenny Kennedy. 2021. *The smart wife: Why Siri, Alexa, and other smart home devices need a feminist reboot.* Mit Press.
[72] Annapoorani Subramanian, Khushi Akhoury, Pooja Chitravelan, Ansu Anna Moncy, Varsha Jayaprakash, Reet Singh, and Sujatha Manohar. 2023. Smart Homes: Is It a Luxury Anymore? *Internet of Things: Applications for Sustainable Development* (2023), 17.
[73] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2020. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 4, Article 153 (sep 2020), 23 pages. https://doi.org/10.1145/3369807
[74] Heather L Turner, Jacob van Etten, David Firth, and Ioannis Kosmidis. 2020. Modelling rankings in R: the PlackettLuce package. *Computational Statistics* 35, 3 (2020), 1027–1057.
[75] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 129–139. https://doi.org/10.1145/2632048.2632107
[76] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 4, 15 pages. https://doi.org/10.1145/2335356.2335362
[77] Rosa Van Koningsbruggen, Sujay Shalawadi, Eva Hornecker, and Florian Echtler. 2022. Frankie: Exploring how Self-Tracking Technologies can go from Data-Centred to Human-Centred. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia (MUM '22)*. Association for Computing Machinery, New York, NY, USA, 243–250. https://doi.org/10.1145/3568444.3568470
[78] Ari Ezra Waldman. 2018. *What Do We Mean by "Privacy"?* Cambridge University Press, 11–46.
[79] Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. 2018. Enabling Live Video Analytics with a Scalable and Privacy-Aware Framework. *ACM Transactions on Multimedia Computing, Communications, and Applications* 14, 3s (June 2018), 64:1–64:24. https://doi.org/10.1145/3209659
[80] Yang Wang. 2018. Inclusive Security and Privacy. *IEEE Security & Privacy* 16, 4 (2018), 82–87. https://doi.org/10.1109/MSP.2018.3111237
[81] Maximiliane Windl, 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)*. Association for Computing Machinery, New York, NY, USA, Article 70, 16 pages. https://doi.org/10.1145/3544548.3581167
[82] Richmond Y. Wong, 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* (<conf-loc>, <city>Pittsburgh</city>, <state>PA</state>, <country>USA</country>, </conf-loc>) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 1093–1113. https://doi.org/10.1145/3563657.3596012
[83] Paweł W. Woźniak, 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)*. Association for Computing Machinery, New York, NY, USA, Article 719, 13 pages. https://doi.org/10.1145/3411764.3445299
[84] Takayuki Yamada, Seiichi Gohshi, and Isao Echizen. 2013. Privacy Visor: Method for Preventing Face Image Detection by Using Differences in Human and Device Sensitivity. In *Communications and Multimedia Security (Lecture Notes in Computer Science)*, Bart De Decker, Jana Dittmann, Christian Kraetzer, and Claus Vielhauer (Eds.). Springer, Berlin, Heidelberg, 152–161. https://doi.org/10.1007/978-3-642-40779-6_13
[85] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019. *Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart Homes.* Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300428
[86] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 59:1–59:24. https://doi.org/10.1145/3359161
[87] Ali Zaidi, Rui Yang, Vinay Koshy, Camille Cobb, Indranil Gupta, and Karrie Karahalios. 2023. A User-Centric Evaluation of Smart Home Resolution Approaches for Conflicts Between Routines. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 1, Article 45 (mar 2023), 35 pages. https://doi.org/10.1145/3581997
[88] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
[89] Fengjiao Zhang, Zhao Pan, and Yaobin Lu. 2023. AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home. *Information & Management* 60, 2 (2023), 103736. https://doi.org/10.1016/j.im.2022.103736
[90] Hui Zhang, 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)*. Association for Computing Machinery, New York, NY, USA, 368–378. https://doi.org/10.1145/2531602.2531685
[91] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (Nov. 2018), 200:1–200:20. https://doi.org/10.1145/3274469
[92] Shoshana Zuboff. 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.

A SURVEY 1: SCREENER FOR GETTING TARGET SHC USERS

A.1 Demographics

(1) What is the highest degree or level of education you have completed?
(2) What type of home do you currently live in? (e.g., apartment, shared living, etc.)
(3) How many people are living in your household?
(4) How many children do you have?
(5) Do you also live with senior citizens?

A.2 Context and Smart Home Camera Use

(1) What other smart home devices do you own in addition to smart home cameras?
(2) What do you use your smart home camera for?
(3) How long have you been using your smart home camera?
(4) How often do you use smart home cameras?
(5) Do you use more than one smart home camera?
(6) What is/are the model of your smart home camera(s)?
(7) Where have you located your smart home camera in your home? (e.g., living room)
(8) Do you move your smart home camera within the home?
(9) In your own words, have you taken any steps to increase privacy, security, trust and control of your smart home cameras?
(10) Have you ever felt the need to cover your smart home camera lens to feel more comfortable?
(11) Can you think of times where you thought you wished you had covered the camera lens?
(12) Please breifly describe the situation when you wished you had covered the camera lens?

A.3 Smart Home Camera User type

(1) How was the smart home camera introduced to your home?
(2) How did you learn to use the smart home camera?
(3) How was the smart home camera set up at home?

A.4 Privacy Perception

Each statement was rated on a five-point Likert scale ranging from strongly disagree to strongly agree.

(1) I am concerned that smart home cameras may use my personal information for other purposes without notifying me or obtaining my authorization.
(2) When I give personal information to use smart home cameras, I am concerned that the cameras may use my information for other purposes.
(3) I am concerned that smart home cameras may share my personal information with other companies or people without my authorization.
(4) I am concerned that smart home cameras are collecting too much information about me.
(5) I am concerned that smart home cameras may monitor my activities on my smartphone.
(6) I feel that as a result of using smart home cameras, others know more about me than I am comfortable with.
(7) I believe that as a result of using smart home cameras, the information about me that I consider private is now more readily available to others than I would like.
(8) I feel that as a result of my using smart home cameras, information about me is out there that, if used, will invade my privacy.
(9) Companies seeking information online should disclose the way the data is collected, processed and used.
(10) A good consumer privacy policy should have a clear and conspicuous disclosure.
(11) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

B SURVEY 2: PERCEPTIONS OF CREEPINESS AND TRUST

You will be shown 4 different videos of smart home cameras and then asked to rate statements based on the video watched.

For each of the four vignettes, the following questions were asked. Each statement was rated on a five-point Likert scale ranging from strongly disagree to strongly agree.

B.1 Perceived Creepiness

(1) I think that the designer of this smart home camera had immoral intentions.
(2) The design of this smart home camera is unethical.
(3) Using this smart home camera at home will make other people laugh at me.
(4) I would feel uneasy using this smart home camera at home.
(5) This smart home camera looks bizzare to me.
(6) This smart home camera looks as expected.
(7) I don't know what the purpose of the smart home camera is.
(8) This smart home camera has a clear purpose.

B.2 Perceived Trust

(1) I believe that there could be negative consequences when using this smart home camera.
(2) I feel I must be cautious when using this smart home camera.
(3) It is risky to interact with the smart home camera.
(4) I believe that this smart home camera will act in my best interest.
(5) I believe that this smart home camera will do its best to help me if I need help.
(6) I believe that this smart home camera can understand my needs and preferences.
(7) I think this smart home camera is competent and effective.
(8) I think that this smart home camera performs its role very well.
(9) I believe this smart home camera has all the functionalities I would expect.
(10) I use this smart home camera, I think I would be able to depend on it completely.
(11) I can always rely on this smart home camera.
(12) I can trust the information presented to me by this smart home camera.

B.3 Qualitative Responses

Imagine in the future, smart home devices with cameras could look and behave in a certain way that is suitable to your household values.

How would you rank the four choices for smart home cameras?

Would you like to provide a detailed opinion on the choice you made? We will verify your answers manually and offer you a bonus payment (+1 EUR).

(1) Please motivate why you ranked the smart home cameras in that way.
(2) How likely is that you would buy one of the smart home cameras, or change the smart home cameras you have?

(3) How do these smart home cameras affect you? E.g. like being watched by the smart home camera. Would you have a negative or a positive feeling as the end result of using these smart home cameras?
(4) How hard or easy is it to understand these smart home cameras? E.g. the status of the camera. And why?
(5) How do these smart home cameras support or not support the comfort of other household members? (E.g. Children, Senior Citizens, Guests)