Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras

Neilly H. Tan
Human Centered Design and Engineering, University of Washington, Seattle, Washington, United States
nhtan@uw.edu

Richmond Y. Wong
Center for Long-Term Cybersecurity, University of California Berkeley, Berkeley, California, United States
ryw9@berkeley.edu

Audrey Desjardins
School of Art + Art History + Design, University of Washington, Seattle, Washington, United States
adesjard@uw.edu

Sean A. Munson
Human Centered Design and Engineering, University of Washington, Seattle, Washington, United States
smunson@uw.edu

James Pierce
School of Art + Art History + Design, University of Washington, Seattle, Washington, United States
jjpierce@uw.edu

ABSTRACT

The increased adoption of smart home cameras (SHCs) foregrounds issues of surveillance, power, and privacy in homes and neighborhoods. However, questions remain about how people are currently using these devices to monitor and surveil, what the benefits and limitations are for users, and what privacy and security tensions arise between primary users and other stakeholders. We present an empirical study with 14 SHC users to understand how these devices are used and integrated within everyday life. Based on semi-structured qualitative interviews, we investigate users' motivations, practices, privacy concerns, and social negotiations. Our findings highlight the SHC as a perceptually powerful and spatially sensitive device that enables a variety of surveillant uses outside of basic home security—from formally surveilling domestic workers, to casually spying on neighbors, to capturing memories. We categorize surveillant SHC uses, clarify distinctions between primary and non-primary users, and highlight under-considered design directions for addressing power imbalances among primary and non-primary users.

CCS CONCEPTS

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

KEYWORDS

Internet of Things (IoT), smart cameras, surveillance, privacy, personal data, tracking, design

CHI '22, April 29–May 05, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3517617

ACM Reference Format:
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 *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29–May 05, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3491102.3517617

1 INTRODUCTION

Variously referred to as smart products, connected devices, and Internet of Things (IoT) technologies, the range and quantity of networked, internet-connected, and data-driven things appears to expand daily. While today we have smart speakers, watches, doorbells, locks, and televisions, tomorrow we may find ourselves regularly interacting with smart kitchens, sidewalks [59], showers, and toilets [98]. These technologies may provide us better ways of living, working, playing, creating, and caring for others. Their use, however, also accompanies a myriad of privacy concerns, security vulnerabilities, and potentials for bias and discrimination (e.g., [22, 94, 138]) that are still emergent, evolving, and woefully unresolved. Prior work has provided qualitative empirical studies of smart devices in general [25, 32, 77, 90] and of specific sensing devices—including smart speakers [6, 14, 16] and activity trackers [75, 91, 93]. In this paper, we focus on one device that has not yet been given this same level of focused, qualitative, and design-oriented investigation: standalone consumer smart home cameras (SHCs).

Smart home cameras are one of the most popular and growing categories of consumer smart home and automation products. Often these devices are marketed as smart home *security* cameras or ***surveillance*** cameras. However, these devices are also marketed and used as more than devices for deterring or catching intruders. For example, Google Nest and Amazon Ring promotional materials depict use cases for watching pets, monitoring packages, and greeting guests (Figure 1). A Nest marketing campaign even created an official award contest, dubbed "The Nesties," that invited users to submit funny and awe-inspiring video clips for award categories such as "Best Dog in a Lead Role" [27]. These marketing materials

suggest benefits that extend beyond conventional home security and into the realms of entertainment, productivity, social media, and meaning-making.

Our research seeks to understand how people actually use smart cameras, and whether these uses align or diverge with promoted use cases. We see hints of a variety of uses extending beyond conventional home security across social media, market research, and news reporting. In popular culture, such clips occasionally go viral and are reported in news media—such as a heartwarming video of a young trick-or-treater filling an empty Halloween bowl with candy for other children [82] or a video of a housecat successfully scaring off a coyote [63]. Alongside heartwarming and jaw-dropping smart home camera videos, these devices have also reportedly been used to spy, prank, threaten, and abuse (e.g., [21]). Somewhere in between these two extremes, prior market research suggests many people use SHCs to watch pets, guests, and family members [139].

In the future, there is every reason to expect that we will see more smart cameras. Unit sales for "smart home surveillance cameras" are expected to grow from 54 million in 2018 to 120 million in 2023 [1], a total that excludes devices with similar functionality such as baby monitors, action cameras, and smart camera capabilities built into smartphones and other devices. In 2016, SHCs generated more retail revenue than any other home automation category and were the most common entry point to the smart home market [139].

Smart home cameras are an inherently surveillant technology that can be used to monitor, track, and record other people, often with little awareness or consent. Beyond simply recording video or audio, machine learning (ML) and other forms of image, video, and audio analytics enable SHCs to infer insightful and revealing information such as recognizing motion, people, faces, animals, vehicles, and noises including breaking glass and smoke alarms. Beyond consumer SHCs specifically, digital imaging and video analytics technologies are seen as one of the most transformative emerging technologies with applications that include driverless cars, predictive policing, patient monitoring, and neuromarketing. Many cultural flashpoints emanate from these technologies, notably concerns with facial recognition technology and implicit biases [36]. While not the direct focus of this study, this broader array of applications and issues provides additional motivation for our work, as our study may shed secondary insights into design opportunities, limitations, and concerns regarding smart cameras and image/video analytics more generally.

Against this backdrop, we present findings from 14 qualitative interviews with smart home camera users in the United States about their uses and experiences with these devices. Our study is motivated by the following questions:

- **Q1. How and why do people use SHCs?** SHC promotional materials and market research suggest that people use SHCs for reasons beyond deterring intruders including monitoring pets, kids, and family [130, 139] (and see Figure 1). Our study set out to determine if these and other such uses are occurring or not, and why.
- **Q2. What, if any, concerns do SHC users have with regards to privacy, security, trust, and control of these devices?** Prior research finds that many consumer smart home device users generally express high degrees of trust in manufacturers and service providers to protect their privacy and security [137], even as these remain a critical concern for researchers, policymakers, and governments.
- **Q3. How are people using SHCs in relation to others—including the monitoring or surveilling of family, neighbors, guests, workers, and passersby?** Prior research has found tensions between primary and secondary users of some smart devices [80], including perspectives of bystanders [133] and usees [11]. Our study is designed to better understand how primary users relate to other subjects affected by their SHCs. To a lesser degree, our study also directly investigates the perspectives of non-primary users affected by SHCs.
- **Q4. How might we approach the design of SHCs and similar technologies to better address the needs of both primary users who own and operate these devices, and other people who are surveilled and otherwise affected by these devices?** Current usable privacy and security approaches focus on notice-and-consent [114, 115] and individual user interface controls (e.g., [2]). Yet both have been shown to have significant limitations, as privacy policies are rarely read and security warnings are often ignored. These approaches are even less applicable when considering bystanders and usees who, by definition, have limited, if any control of the system.

This paper thus makes three core contributions across HCI and interaction design, and their intersections with discourses of data privacy, security, trust, surveillance, and power. First, we provide qualitative descriptions of SHC users' motivations for adopting the devices, and their actual uses and levels of comfort with these surveillant technologies to support a variety of everyday activities. Second, based on our findings we contribute two sets of concepts to aid designers and researchers with studying and improving SHCs and similar technologies. We highlight the need to treat smart cameras and other spatially sensitive and perceptually powerful technologies differently because their capabilities inherently extend across large areas and distances, and inevitably affect the privacy and security of other stakeholders. Regarding SHC and smart device users, we clarify important distinctions between primary and non-primary users, and between frontend and backend users. *Non-primary users*—such as housemates, neighbors, domestic workers, or passersby—may interact with SHCs but do so with comparatively limited awareness, consent, and control compared to the *primary users* who own and operate them. Adding a second layer to this distinction, a *backend user*—such as a company or hacker—accesses a smart device that is owned and operated by a primary *frontend user*, who is oblivious to or only peripherally aware of the backend user and their uses (e.g., selling their data to third-party advertisers). These distinctions are indispensable in clarifying the stakeholders and stakes involved in the complex network of interactions surrounding SHCs and always-on devices.

Finally, we contribute a set of design insights and opportunities informed by the preceding contributions. At a basic level, we foreground a core ethical design dilemma: how—and to what extent—to support the needs and desires of primary users (and paying customer) in ways that are not invasive and harmful to non-primary

users. While this dilemma represents a complex, wicked problem [104] that defies any clear solution, we outline several promising and under-considered directions for future design activity, including non-primary user side controls, shared and negotiated controls, and latent interactive controls and safeguards.

2 BACKGROUND AND RELATED WORK

Our study sits at the intersection of four areas: (1) consumer IoT and smart home devices, (2) privacy, security, and surveillance studies, (3) design research, and (4) what some have recently referred to as FATE: fairness, accountability, transparency, and ethics in artificial intelligence (AI), machine learning (ML), and data science.

2.1 Related Empirical Studies in IoT

Recent work has empirically studied how people use a range of IoT devices, including voice assistants and smart speakers [6, 14, 16], smart home automation [25, 32, 77, 90], home resource management tools [132], and experimental design prototypes [53, 127]. Other related areas of study include telepresence [73, 103] and video communication [23, 85]. IoT researchers have also notably studied issues of privacy and security [136, 137] in the context of Internet connected toys [89] and smart speakers [80, 86]. Some researchers have evaluated privacy perspectives with existing and novel camera technologies. For instance, Machuletz et al. discuss how the use of integrated webcam covers is dependent on user's attitudes and perceived control over maintaining their privacy [85]. Hoyle et al. also examine how wearable camera users weigh factors such as time and location to manage their privacy and to determine the sensitivity of footage captured on their lifelogging device [69].

Other empirical studies with IoT have specifically analyzed surveillance technologies. For instance, Kozubaev et al.'s work with smart technology in public housing addresses the effects of surveillance cameras in semi-public spaces, and they discuss how surveillance technologies can further exacerbate racial and economic inequalities [78]. Some have critically studied carceral surveillance technologies and individuals living under state surveillance [76, 97, 107, 121]. In [97], Owens et al.'s investigation on the surveillance of communication with family members of incarcerated people reveals participants' varied understandings of the extent that they are being surveilled by certain technologies, such as cameras for monitoring in-person visitation. They also assess participants' privacy concerns, attitudes, and assumptions amidst increased surveillance (highlighting the relational consequences of increased forms of monitoring and surveillance like location tracking, for example). Under admittedly different contexts, we explore similar concepts regarding users' assumptions and dynamic privacy dependencies with the smart camera as a surveillance technology. We further consider how commercial applications of pervasive technology systems afford increasing surveillance uses by creating a panoptic gaze through enabling novel sensing mechanisms.

Researchers have additionally investigated smart home and consumer IoT technologies with an eye toward the effects of surveillance on nearby others. Prior work has pointed to potentially invasive effects of common smart sensing devices on bystanders [48, 133] and non-primary users [80, 102]. Other work has studied bystander privacy in public spaces with phones and smart glasses [41, 113] and with drones [134]. For example, with augmented reality glasses, bystanders express an interest in mechanisms for blocking recording and for supporting permission negotiations [41]. Likewise, bystanders' reactions to publicly being recorded are dependent on multiple factors, such as their gender, surroundings, and what activity is captured [113]. And as smart technologies blend the boundaries of public and private distinctions in the home [33, 67], it is further necessary to understand bystander privacy in domestic environments.

2.2 Power Dynamics and Ethical Tensions

As such, IoT studies find privacy tensions arise between primary and non-primary users, and foreground unequal access and conflicting interests [33, 136]. In the context of smart speakers and home voice assistants, Lau et al. [80] discuss privacy tensions between users and incidental users of smart devices placed in common communal areas such as the living room. Pierce's design inquiry unpacks similar tensions in smart home cameras, highlighting "hole-and-corner" applications in which users' data and interactions are downplayed to them [101]. This can lead to harmful and controversial uses, as Pierce describes in a speculative scenario with emotion tracking regulation for nannies, and is aligned with other work that addresses how abusers can exploit digital technologies in intimate partner violence contexts [47, 81]. Additionally, recent work highlights a need to study privacy and security practices and experiences of diverse and vulnerable users, including children [89], Airbnb guests [87], older adults [18, 40, 48], and subjects of cyber harassment, domestic violence, and hate speech [13, 20, 34, 47, 88]. While work in privacy and security has begun to address the privacy needs of different populations (e.g., [44, 66, 105, 109, 128]), such understandings are still nascent, incomplete and, in many cases, have not been translated into adequate solutions and recommendations.

More generally, a broader discourse concerning the ethics of IoT, AI, and surveillance has emerged within HCI and science-technology-society (STS), among other adjacent fields. With regards to privacy and security, scholars have theorized ways of understanding threats and harms of digital data in terms of contextual integrity [94], surveillance capitalism [138], racialized surveillance [22], and the effects of digitizing video surveillance [60]. Sociotechnical scholars discuss notions of governmentality, accountability, and ethics with algorithmic [8, 54, 79] , smart sensing [35, 58] and cloud-based systems [7, 70]. Furthermore, the data-driven and pervasive modes of computing that are central to IoT can obscure legibility to its users. Recent efforts for open and fair IoT data literacy [38, 49] raise concern about the pervasive connectivity of IoT devices, and how IoT can amplify challenges related to privacy and ethics [17, 35, 111]. A prominent line of STS and cultural studies scholarship has challenged scientific and engineering understandings of data as objective or neutral, describing instead how it may be uncertain [15, 43, 62], heterogenous [5, 42], and local [84].

2.3 Studies Involving Home Security Cameras

Various research on home surveillance and internet-connected cameras have prefigured many frontiers for today's complex smart camera interactions. For example, prior work with internet-connected home security cameras and smart locks suggests ways to alleviate

potential privacy concerns from teens and parents through outsourcing the auditing of home entry data logs to companies or through technology-assisted facial recognition features [123]. Early research directions also explore the concept of sharing camera data between neighbors [24]. Furthermore, studies with home surveillance cameras reveal how initial anxieties and concerns regarding privacy gradually wane over time as users become accustomed to their presence [96]. As the smart camera has since evolved with robust tracking, sensing, and data sharing capabilities, these features further complicate past findings about the potential ways that surveillance cameras can affirm or realign power relations within households and communities.

However, despite the vast empirical research on IoT, surveillance technologies, and domestic sensing and security devices, our literature review found few examples of qualitative empirical studies primarily focused on smart home cameras. Ahmad et al. [4] examine tangible privacy perceptions with non-owners of the Nest security camera and the Amazon Echo Show, a smart voice assistant with video sensing capabilities. Their interviews demonstrated a general uncertainty regarding devices' on and off states, which can be further complicated with possible tensions of navigating interpersonal solutions for preserving bystander privacy without tangible feedback that the device may still be recording them. A self-use study of smart cameras by Pierce et al. [100] identified several prominent trust and controls issues for both primary and non-primary users, including "not trusting it's OFF," "forgetting it's ON," and "lack of control options"—such as unreliable indicator lights, lack of physical controls, and lack of granular controls. We extend findings about bystanders' perceptions of video and audio recording sensing devices through specifically analyzing primary users' motivations and uses across various smart security cameras, in addition to their perceptions about the social dynamics of operating such devices.

Other empirical investigations with the smart camera examine its risks alongside other IoT or internet-connected devices [29, 55, 87, 118]. These studies describe the smart camera with respect to the different power relations that it enables amongst other smart home devices in the context of families, multi-user home settings, and in temporary homes between Airbnb hosts and renters. For example, Chalhoub et al.'s longitudinal analysis of smart systems highlights how repurposing such technology for other purposes can lead to potential misuse by exacerbating power imbalances within households [29]. Mentioning two households who have repurposed their smart cameras for entertainment, parenting, and streaming uses, they discuss how a loss of control and debates over ownership of video footage can arise between different family members.

Likewise, researchers have described different methods for confronting or diffusing these power dynamics through how such technologies novel interpretations and feminist orientations [68, 118]. At the company level, researchers find that one goal of smart device designers is to ensure that the technologies like smart cameras are not perceived as "creepy" or "intrusive" [28]. Some of these emerging design potentials, including dystopian provocations of surveillance in smart cameras, have been explored through design research approaches such as design inquiry [101] and research through design (RtD) [102, 120, 127].

As a result, our study calls attention to the standalone smart camera as a unique form of IoT that requires dedicated analysis. Specifically, our contributions of different surveillance categories and power asymmetries complement related work with understanding complex social dynamics surrounding IoT devices, from intra-household relationships to smart home companies. Furthermore, although privacy and security represent a focus of our study, it is not the sole focus. We seek to more broadly understand the various uses and experiences of these increasingly popular, pervasive, and potentially invasive devices. And while our work is informed by and directed towards HCI design research and RtD, our research adopts a qualitative empirical approach to investigate user experiences and practices, along with social tensions and power dynamics, connected to the consumer smart home camera.

3 METHODS

We conducted semi-structured interviews over Zoom (with 1 in-person interview) with 14 geographically and experientially diverse smart home camera users in the United States. This study was approved by our university's Institutional Review Board, and participants gave formal consent to participating in our study before engaging in the interview. Interviews were 60-90 minutes each, and participants were compensated $50. In these semi-structured interviews, we asked participants about their experiences, thoughts, and current practices with smart cameras. We discussed their use cases, mental models, household dynamics, and other factors they consider when interacting with cameras. With each participant, we conducted a device tour—either virtually or, in one case, in-person—where participants walked us through the different smart cameras in their home, discussing the reasons why they obtained the cameras, where they placed them, and how they used them. Beforehand, we asked participants to send us photographs of their devices in context (in lieu of any potential technical difficulties with conducting the device tour over Zoom). After, we probed further about participants' data practices, assumptions, and privacy practices. Examples of interview questions include: "*What kinds of information do you collect through or with this device?*", "*Have you ever shared videos or information from your camera with others? If so, what did you share and why?*", "*What do you do when guests or others come over?*", and *"Have you ever had an argument over the device? With neighbors, family members, or others?"*.

3.1 Study Participants

We recruited participants from across the United States through social media posts, online forums, and email lists such as posts on smart home camera subreddits and Craigslist. We selected participants based on criteria from our screener survey. We generally sought participants with more than one camera, and with variance across several categories including age, race, number of cameras, living situation, location (rural versus urban), level of engagement (casual users, new users, sustained users, power users), and variety and regularity of reported uses. Our investigation also included two non-primary users—users who interacted with SHCs, but who did not directly install the cameras themselves. We provide an overview of our participants in Table 1.

Table 1: Overview of participants, cameras, and their households

ID	Cameras owned	# of SHCs	Other Household Members	Location (self-described)	Ethnicity (self-described)	Age	Gender	Individual Income Level
P1	Wyze Cam, Google Nest Cam	2	2 (Parents, ages 80 & 70)	Small city, middle of urban and suburban	Asian	37	Male	$50-$100k
P2	Wyze Cam; Ring floodlight Cam	2	1 (Spouse)	Densely populated suburb	White	30	Male	$100-$150k
P3	Nest outdoor security Cam	1	1 (Mother, age 43)	Suburban	Black	19	Female	$50-100k
P4	4 Wyze Cams, Ring doorbell, Wisenet security Cam	6	2 (Husband, age 62; Daughter, age 36)	Suburban	N/A	59	Female	N/A
P5	Google Nest Cams	4	3	Big city	Black/African American	33	Male	$100-150k
P6 [a]	N/A	N/A	1 (age 31)	Big city/ Suburban	White	25	Female	$50-100k
P7	Nest Cam	1	1 (age 29)	Suburban	White	64	Female	Prefer not to share
P8	Wyze Cams ~8, Nest Doorbell Cam	8	2 (1 adult, mid-30s; 1, age 8)	Suburban	N/A	35	Female	Prefer not to share
P9	2 Ring Cams	2	2 (age 35; age 3)	Suburban	Hispanic	36	Male	$50-100k
P10	2 Ring Doorbell Cams, 3 Ring Stick Up Cams	5	5 (ages 71, 45, 12, 12, 12)	Midsize to larger city	Hispanic white	46	Female	$50-100k
P11	2 Amcrest, 17 Eufy, 16 Lorex,	5	4	Rural	White	41	Male	$100-150k
P12	Google Nest Cam IQ Indoor	1	3 (Husband, aged 30; Caregiver, age 25; Child, age 3)	Big city	African American	27	Female	$50-100k
P13	Carson	1 [b]	n/a (lives alone)	Urban	Black	31	Female	$10-50k
P14	Samsung	1	3 (ages 16, 13, 54)	Urban	Black	36	Female	Below $10k

[a] This participant does not own smart cameras but is surveilled by them at work, as a delivery driver, and at home by her neighbors.

[b] This smart home camera was installed in her apartment building.

3.2 Analysis

Data analysis was an ongoing, iterative process throughout the course of the study. Field notes were reviewed immediately following an interview and tentative insights and themes noted in reflective field logs and memos [57]. The team met periodically to debrief, share notes, and generate and record tentative themes.

We transcribed all our interviews using the transcription service Temi. Following transcription, we conducted analysis according to a modified grounded theory coding scheme, overall employing an iterative process of searching for emergent patterns and themes [92]. Once we had completed all interviews, we began by initially coding data according to emergent themes and guided by our memos. We then refined and organized these codes according to larger thematic categories. More specifically, we first focused on clustering participant descriptions of their SHCS uses and later, by emergent overarching categories (e.g., "gaining a better view", "spotting animals", "keeping an eye on kids", "watching over loved ones"). After solidifying these initial categories, we iteratively coded transcript data to eventually arrive at high-level themes, including categories of use, surveillance, trust, and concern for others. Writing and sharing the themes within our research team constituted a final stage in our analysis.

During the course of this study, we also reviewed hundreds of product instructional and promotional images (see Figure 1), monitored our local Ring Neighbors and Nextdoor social media apps (where users frequently share and request video footage pertaining to incidents such as minor trespassing, stalking, burglaries, and package thieves, also known as "porch pirates"). We also purchased, used, and familiarized ourselves with several smart cameras, including the Nest Indoor, Nest IQ Indoor, Wyze Indoor, Yi Indoor, Amazon Ring doorbell, and Blink smart home cameras.

4 STUDY BACKGROUND AND OVERVIEW

Here, we present an overview of smart cameras and our study findings. To aid the reader in contextualizing our findings, we offer a short primer on the form, function, and operation of the SHC products used by our participants. While these features represent the "state of the art" at the time of this study, it is important to note that the functional offerings of these and related devices will continue to expand significantly—particularly with regards to object recognition capabilities (e.g., "animal seen" and "package removed" alerts). Following this guide, we then outline a high-level summary of the various key concepts from our findings, including various categories of SHC use and everyday surveillance.

4.1 Product Onboarding: A Short Guide to Smart Home Cameras

Smart home cameras offer users a variety of novel features, the most common of which include cloud recording, cloud-based video histories and timelines, smart alerts with motion detection, real-time video and audio feeds, and two-way voice intercom communication. Some SHCs offer motion detection, object detection, person detection, and facial recognition features that identify familiar and unfamiliar faces. Additionally, some SHCs allow users to set activity zones to focus these filters on specific areas, while ignoring others.

In contrast to older video security surveillance technologies, SHCs are supported by cloud-based applications that enable live video feeds, automated monitoring, and simplified review and storage capabilities. A paid subscription upgrade is often required to unlock some of these features. The unique cloud components and intelligent detection features of SHCs increase the functionality of home security cameras by providing the ability for users to monitor different facets of their environment through a smartphone app and receive automated notifications when events like motion or unfamiliar faces are detected. One major advertised value of SHCs are relevant activity notifications, such as a person making a loud noise, thus relieving users of a need to constantly monitor or painstakingly review hours of video footage.

SHCs exist in a variety of form factors, including indoor, outdoor, and doorbell cameras. Others include Pan-Tilt-Zoom (PTZ) features that integrate with motion detection (e.g., the Wyze Cam Pan), and anthropomorphic, decorative, or camouflaged camera housings (See Figure 2, lower right, for an example of a camera decorated with a hat). Most are distinguished by their small and sleek design, often blending into the environment (Figure 1).

4.2 Findings Overview

We organize our findings into three sections. First, we describe how and why participants use smart home cameras, with an emphasis on the range of uses and motivations. We then extend these findings to characterize them as surveillant uses. See Table 2 for a summary table of the various key categories of use and surveillance we identify. Finally, we refine our analysis of surveillance by reporting on types of asymmetric user relations we uncovered with significant implications for privacy, security, trust, and power: frontend versus backend uses, and primary versus non-primary users.

5 MORE THAN CAMERAS, MORE THAN HOME SECURITY DEVICES: HOW PRIMARY USERS ARE USING SMART HOME CAMERAS

In this section, we describe the range of smart home camera uses reported by participants. We find that while many users were initially attracted to smart home security cameras for a specific use—often through specific home safety or security applications—all participants reported using these devices in multiple ways to support a wide range of everyday activities. Commonly described conventional home security and safety applications included catching and deterring intruders, thieves, vandals, and negligent caretakers, as well as providing general "peace of mind" (P4), "just in case anything suspicious happens" (P9). While most participants cited these types of conventional home security and safety applications as an initial, and often primary, motivations for adopting SHCs, all participants mentioned engaging in many additional activities with their SHCs such as checking in on pets, greeting and receiving guests, confirming and managing deliveries, keeping an eye on kids, casually spying on neighbors, and reviewing footage of oneself, others, their home, and their neighborhood out of curiosity or without a clear, singular aim.

To better understand this range of uses, we identify several general smart camera capabilities that surfaced across participants, and

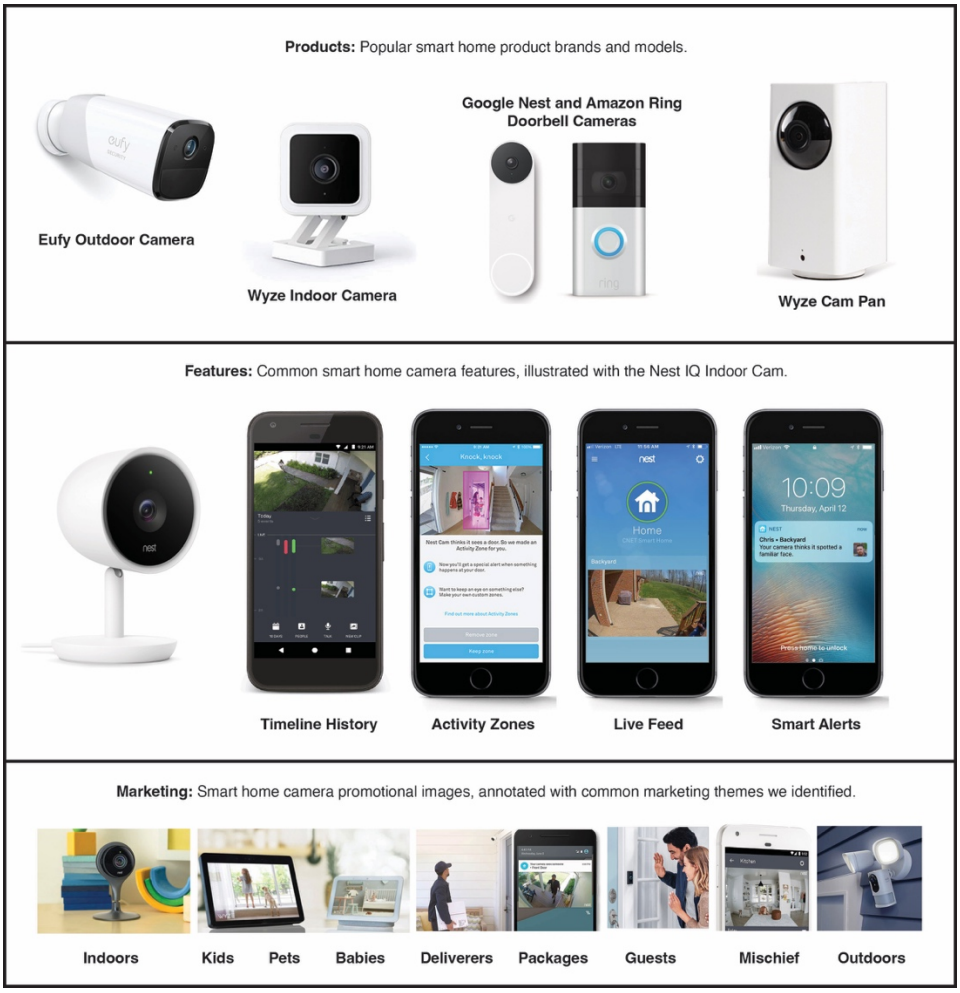

Figure 1: Example SHC products, features, and marketing depictions. Top row: Several popular brands of smart cameras used by participants in our study, including the Eufy outdoor camera, Wyze indoor camera, Google Nest and Amazon Ring doorbell cameras, and the Wyze Cam Pan, which can be rotated remotely from the app. Middle row: Several popular and innovative SHC features, like the timeline history view, activity zones, live feed, and smart alerts—all accessed via the manufacturer's smartphone app. Bottom row: Several official promotional images portraying various marketed use cases indoors, with kids, pets, babies, package deliverers, guests, funny moments (a child attempting to steal a piece of cake), and outdoors.

which enable HCI researchers and designers to better understand the full extent to which individuals use these systems. First, we identify cameras as **extended sensory perception** devices, based on the basic capabilities participants described using. We then report four additional, action-oriented categories of use enabled by this extended sensory perception: **behavioral deterring**, **communicating**, **documenting**, and **device actuating**. We conclude by describing some of the latent perceptual, actional, and affective effects of smart home cameras, namely avoiding SHC sensor fields, feeling pressure from SHC surveillance, and acclimating to SHC surveillance.

5.1 Smart Home Cameras as Extended Sensory Perception Devices

Below, we present several examples depicting how participants commonly use smart home cameras to extend their 'naked' sensory perception [71] of their surroundings. In these sections, we first discuss several directed modes of extended sensory perception, wherein individuals monitor camera data with a relatively clear intention or expected outcome. We report on three sets of directed engagement: anticipatory monitoring, focal monitoring, and retrospective review. In contrast to these directed forms of engaging with SHCs, we also discuss several examples of undirected monitoring and reviewing, in which participants engage with camera data without a clear or singular purpose. Then, we discuss how participants describe what we refer to as the *mere-potential* for

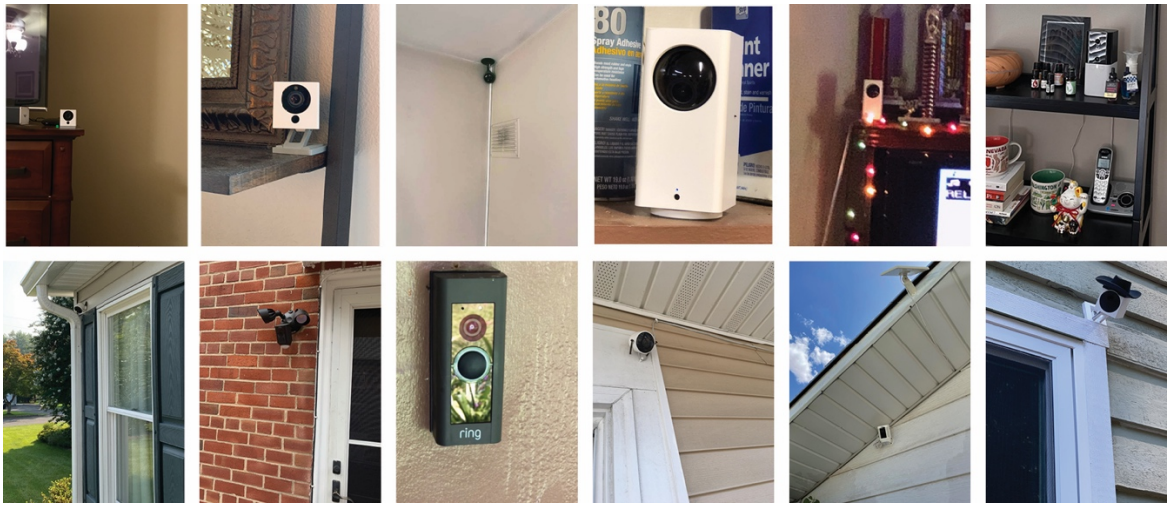

Figure 2: Examples of participants' indoor, outdoor, and doorbell smart cameras. The top row of images depicts various indoor camera placements, and the bottom row depicts outdoor camera placements. Notable images include a camera mounted upside down on the indoor ceiling, a camera placed among other domestic objects on a bookshelf, and an outdoor camera adorned with a small, decorative cowboy hat.

Table 2: Summary of Key Categories of Surveillance and Monitoring

Types of extended sensory-perceptual monitoring in smart cameras (see Section 5.1)	
Anticipatory monitoring (Watching over and watching out for)	Using smart home camera systems to remotely monitor the environment to watch out for specific events (e.g., keeping an eye on children elsewhere, being aware if a loved one falls, or monitoring package deliveries).
Focal monitoring (Looking into and getting perspective)	Attentively observing live video or audio to actively monitor events (as opposed to peripherally viewing or momentarily checking footage).
Retrospective review (Knowing and evidencing what happened)	Using the smart camera to review past events to know or evidence what happened. Examples include traffic accidents, thefts, and trespassing; spotting animals; catching negligence or abuse; and settling disputes.
Undirected monitoring (Casually checking, peeking, and spying)	Monitoring without a clear or singular instrumental purpose, such as monitoring driven by curiosity or a desire to connect with others, such as checking on pets and animals or spying on neighbors.
Types of interpersonal and cross-device actuation uses (see Section 5.2)	
SHCs as Behavioral Deterrents	Using the smart camera to deter harmful, improper, annoying, or illegal behavior.
SHCs as Interpersonal Communication	Communicating with visitors and workers, co-dwellers, or pets with the smart camera.
SHCs as Documentation Devices	Documenting smart camera footage for reminiscence, sharing moments, or video requests (e.g., investigating a hit and run).
SHCs as Device Actuation Systems	Configuring the smart home camera to deliver text or email notifications, or to automatically capture certain video/audio.
Types of surveillance in smart home cameras (see Section 6)	
Deterrent and Regulating Surveillance	Surveillance to deter or regulate behaviors (typically of others).
Managerial Surveillance	Surveillance to manage and oversee paid workers, e.g., tradespeople or domestic workers.
Care-based Surveillance	Surveilling loved ones to better care for them, or as an outward expression of care.
Diagnostic and Evidentiary Surveillance	Surveillance to diagnose the cause or effect of an event, or as evidence (often in conjunction with deterrent, managerial, or care-based uses).
Cuing Surveillance	Surveillance to anticipatorily notify users of events that may require specific action, such as receiving a package or greeting a guest.
Aesthetic and Atelic Surveillance	Surveillance because it is intriguing, beautiful, shocking (aesthetic surveillance); and/or without a clear instrumental purpose (atelic surveillance)

Figure 3: Examples of P8's anticipatory monitoring of her child (left) and doorway (right).

monitoring, and mere-potential reviewing to achieve desirable outcomes (e.g., having "peace of mind" or feeling in control of their home).

5.1.1 Anticipatory Monitoring: Watching Over and Watching Out For. Overall, participants described using their SHC systems to watch over loved ones, pets, workers, and areas of their homes while they were occupied with other activities elsewhere. Participants also described using SHC systems to watch out for specific events, such as a loved one falling (P1, P4) or a package arriving (P1, P2, P3, P7, P8, P11, P13). These and other examples of anticipatory monitoring involve the use of SHCs to monitor the environment for specific events. Typically, participants used automated smartphone alerts, such as motion or person detection, to aid in anticipatory monitoring, thus removing the need to focally monitor the live video or audio feeds.

Most cases of anticipatory monitoring we uncovered involved doorbell cameras or cameras directed at outside entryways. Beyond mere awareness, anticipatory monitoring was frequently described as valuable for prompting or cuing users to take specific action or inaction. For example, P8 described regularly using an entryway SHC to receive an indication when a guest is parking or walking up to her doorway so that she can put her dog away before he starts barking. For her, these few additional moments make a big difference as they allow her to prevent her dog from causing a scene and more pleasantly greet a guest. (Note, however, that other participants found that a lag-time of several seconds between event and notification prevented them from responding to certain events; for example, by the time they received an alert someone had already left.)

Another common use of anticipatory monitoring we observed is parents using smart cameras to keep an eye on their children. P10 described how she places an indoor camera near her three kids while working elsewhere around the home because she "doesn't have extra eyes or ears." In such cases, a few participants devised display configurations that allowed them to continuously peripherally watch over their children through the live camera feed while performing other tasks. P8 described and demonstrated how she positioned a Facebook Portal display screen next to her home office work computer to monitor her child playing outside (See Figure 3) — thus creating a glanceable display akin to a virtual window (e.g., [51, 52]).

One participant, P4, uses smart cameras to anticipatorily monitor her husband who has Parkinson's disease. She described how SHCs enable her to keep an eye for any potential falls from a distance, allowing her husband to maintain his autonomy ("without making him think that I'm hovering over him" physically). P4 explained the labor involved with monitoring her spouse before she had cameras:

> "I'd be running drinks to him every 30 minutes. . . I'd say, 'Stay where I can see you!'. . . Or I'd ask my daughter, 'Did Dad come in yet?' It was like, I'd have to search for him. It got kind of nerve wracking, cause I was like, micro-managing his life." —P4

Now with cameras, she says, "I'm [still] micro-managing but it's at ease." Reflecting on the overall value of cameras, P4 expresses,

"All I know is that smart home cameras provide something that I can't—I can't be a watchman 24 hours a day." Thus, anticipatory monitoring mediates a variety of temporal expectations: tracking certain future events (e.g. package deliveries), and managing care and concern around events that may happen (e.g. falls or harm).

5.1.2 Focal Monitoring: Looking into and Getting Perspective. A second mode of engagement with SHCs we observed is focal monitoring, wherein a user attentively observes live video or audio to focally monitor what is happening, rather than peripherally viewing or momentarily checking. Instances of focal monitoring were often described as short duration events, typically just long enough to assess what is happening. For example, participants described scenarios where anticipatory monitoring transitioned to short-duration focal monitoring, such as watching the doorbell camera video long enough to assess who is at the door and determine whether to answer or ignore them. Longer duration viewing was, in general, less mentioned by participants and typically constrained to retrospective review of past data, which we discuss later.

Two participants described exceptional or infrequent acts of focal monitoring that involved longer duration viewing. P8 described how at night she will sometimes hear a noise and then watch the live feeds from their multiple indoor and outdoor cameras to monitor what is happening, even though she "know[s] it's probably nothing" and "it never is [anything of alarm]" P3 demonstrated how she remotely repositions and angles the camera to eavesdrop on conversations outside. Both examples illustrate how SHCs may enable users to gain a better perspective on nearby activities.

5.1.3 Retrospective Review: Knowing and Evidencing What Happened. Participants described many instances where they engaged in retrospective review of video and audio recordings, along with metadata such as timestamps and filtered events (e.g., motion, a person, a loud sound). Later we discuss retrospective reviewing related to reminiscence, managing workers, and curiosity-driven engagement. Below we present several other examples, ranging from serious to playful.

Neighborhood traffic accidents, thefts, and trespassing. Some participants used smart cameras to document, evidence, or solve unexplained crimes. For example, P5 reviewed their SHC video when someone trespassed and tried to break into his house and learned that it was his neighbor's son. He subsequently used this evidence to confront his neighbor.

Spotting animals. Many participants reported spotting animal activity with their smart cameras. Several participants discussed rare and awe-inspiring recordings, including spotting a wolf and coyote on their patio (P11), a bald eagle eating their chickens (P11), and a bear walking through their residential neighborhood (P8). These and other participants typically indicated that animal spotting was a valued and sometimes regular use of their smart cameras.

Catching negligence and abuse. One participant (unnamed for privacy purposes) discussed how she uses the cameras to check up on her daughter and daughter's caregiver. She explained a complicated situation wherein she used her SHCs to identify an act of abuse by the caregiver, which we refrain from detailing for privacy reasons. This participant described how SHCs were especially valuable for monitoring caregivers, to help prevent or identify possible future cases of abuse or negligence.

Settling disputes. In at least three cases, participants reported using smart camera recordings to settle interpersonal disputes with neighbors or family. P11 relayed an initial event where he told his nephew, whom he suspected was lying to him, that they would "check the cameras" to confirm if his side of the story was true. Over time, this became a pattern in which P11 would occasionally threaten his nephew by saying, "let's check the cameras", when, for example, he suspected the nephew was lying about finishing a household chore. P11 later began using this warning with his own children, although he eventually stopped doing so due to conflicted feelings about this emergent SHC use to threaten and settle family disputes: "I didn't want to use [the smart camera] as a weapon."

5.1.4 Undirected Monitoring and Review: Casually Checking, Peeking, and Spying. Participants also described several use cases involving partially or predominantly undirected monitoring and review, which seemed to lack a clear instrumental purpose or outcome. Often participants suggested these were driven by curiosity, a desire to connect with family or pets, or possibly anxiety or habituation. Later we elaborate on these and related uses as aesthetic and atelic surveillance. Below we note two commonly reported areas of undirected monitoring.

Checking on pets and animals. Several participants used SHCs to check on pets (P2, P3, P4, P8, P10), especially when they were away from their homes. A few participants specifically set up additional cameras for this purpose—for example, checking on their puppy while away from work (P2) and monitoring their chicken coop and horses (P11).

Casually spying on neighbors. Participants also described undirected monitoring to casually spy (our term) on neighbors, often described as an accidental or opportunistic activity, rather than premeditated. For example, two participants, P3 and P13, expressed how they semi-regularly liked to listen in on conversations between neighbors, even though they both do not usually talk to their neighbors. P13 referred to this as "people watching" through the smart camera.

5.1.5 Mere-Potential Monitoring and Review: I can—but I haven't. In the uses reported above, participants described actual, immediate engagement with SHC sensor data and visual, auditory, and textual representations thereof. Distinct from, yet intimately related to this *actual* monitoring and reviewing, participants sometimes described a value of SHCs in terms of a *mere-potential* for monitoring or reviewing events that had not actually occurred, had not been captured, or which they had not yet viewed. Participants described the value of these mere-potential sensory-perceptual capabilities when frequently discussing events that might happen: "I *could* use this to check on [if my older dad falls]" (P1); "I saved a lot of footage of [the neighborhood children] coming near my property, *just to have it*, to show ongoing harassment [to police]" (P10) (*emphases added*). Some participants also referenced capturing a single event that validated their installation of the smart camera and their continued use of the device. For instance, P11 explained that he initially installed SHCs for security purposes and, while friends called him "crazy" at first, his cameras transitioned from the mere-potential to actual review of video footage when someone had broken into his home.

A common framework used in qualitative analysis when describing examples of uses and behaviors is to identify mismatches between what participants say they do and what they actually do. We agree, but offer an additional interpretation to this duality: SHC users meaningfully and consciously use the mere-potential for monitoring and reviewing to achieve senses of safety, security, control, and power. Which is to say, *potential* uses appear to be a very real and valuable use of smart cameras, and surveillance apparatuses in general.

5.2 From Personal Extension of Sensory Perception to Interpersonal and Cross-Device Interaction

Our previous examples demonstrated how cameras are used to enhance people's sensation and perception of their environment. In this section, we highlight four additional general capabilities of smart cameras that build upon extended sensory perception in ways that effect specific types of responses in other people or devices: behavioral deterrence, interpersonal communication, documentation, and device actuation.

5.2.1 Smart Home Cameras as Behavioral Deterrents. Unsurprisingly, given the design and marketing of these devices as smart *home security* cameras, one of the most cited uses of smart home cameras among our participants was to deter harmful, improper, annoying, or illegal behavior. Throughout the paper, we report many examples in which participants describe or allude to *behavioral deterrence* as a primary use and value of their SHCs. The most reported target of behavioral deterrents was to inhibit trespassing, intrusion, theft, vandalism, and related forms of harmful activity from predominantly unknown and unexpected persons. Some participants also described using SHCs to deter negative behavior from specific neighbors, family members, guests, and domestic workers. Whereas a parent in our study described SHCs as "extra eyes and ears" (P10), another participant described the devices as a "friendlier" form of "bars on the window" (P9).

To function as an effective deterrent, participants often described the importance of installing cameras with sufficient visibility to deter potential intruders. At the same time, these participants often noted a counterbalancing need for *inconspicuous* placement that does not draw the alarm or disdain of neighbors who might vandalize or negatively judge the SHC owner. P14, for example, feared that if her cameras were too visible then her neighbors might vandalize it. P2, whose camera has a floodlight sensor that lights up at night based on motion, elaborated on how his camera's form factor needed to be conspicuous, not only to deter intruders, but also to visually communicate to others that he was not using it for stealth purposes:

> "The smaller the camera, the more [it's] like a spy or nanny cam. I don't want to be secretly recording anybody and I don't want it to be a surprise. I got the cameras for security. The more obvious that it is, the better security it provides. . . No one's going to walk in and think that there's no camera, it's like this giant light turns on." —P2

These responses suggest a tacit camera placement principle: just conspicuous enough to deter, but not so conspicuous as to stand out in a way that might be negatively perceived. For some participants, this balance was more important than to others.

5.2.2 Smart Home Cameras as Interpersonal (and Interspecies) Communication Devices. Some participants used their smart home cameras to support two-way communication through the built-in voice intercom feature or, in a few cases, in conjunction with smartphone text or voice communication. We found three main groups that participants frequently reported communicating or attempting to communicate with.

Communicating with visitors and workers. Participants described using their SHCs to communicate with delivery workers. This enabled P4, for example, to interact with delivers while she's away from her home; "You can just say, 'Oh, I'm busy right now. I can't come to the door, leave the package on the side."' The ability to communicate via the SHC helped P4 feel more at ease answering the door: "That's one aspect I like about the Ring doorbell. They don't know you're home [you could be communicating with them remotely from anywhere]."

Communicating with co-dwellers. Participants described using the built-in voice intercom in conjunction with the camera to communicate with their kids or spouses, either when they were away from home or in separate rooms. P11 describes how communication with and visibility of his family were primary motivators for adopting indoor SHCs: "So the initial [reason I adopted SHCs] was just, I could hit a button and say 'hi' to my girls. I can hit a button and talk to my wife rather than have to call her. And I like my house. I like my family. It's nice to be able to hit a button and see them." At times, P11 more specifically uses his SHCs to visually check when his kids were not responding to his text messages, and then getting their attention by using it as an intercom. Other participants reported using SHC communication features in playful ways, including using the intercom to scare family members (P9, P10) or pets (P3).

Communicating with pets. Many participants used SHCs to monitor pets, and a few described specific instances of using SHCs to communicate, or attempt to communicate, with pets. P4 communicates with her dog when she is away from home through setting her Echo Show on a chair to check on him: "I can drop in and see my dog, and my dog can see me." Likewise, P3 explained that she uses her Nest Cam "when her cats accidentally leave the house [to] call them in." P3 also described one notable case when she used her SHC to find a lost cat through its audio features, deducing that her cat was in her neighbor's yard through hearing it meow on the camera feed.

5.2.3 Smart Home Cameras as Documentation Devices. Participants further indicated the value of SHCs as documentation tools that enabled them to archive and share recorded events with others. Later, we elaborate on two types of surveillant uses related to documentation: *surveillant memory-making* and *evidentiary surveillance*. We illustrate three specific documentary applications below.

Reminiscence. Several participants described instances where they either deliberately or serendipitously reviewed documented audio and video of their lives in way that facilitated reminiscence—the enjoyable recollection of past events. P11 saved one sentimental

video of his kids and mother-in-law walking together, and P14 described reminiscing on videos captured by her SHC of her and her children on family outings and at neighborhood festivals. These examples recall novel HCI design prototypes for enhancing and supporting reminiscence (e.g., [99, 135]).

Sharing moments. Several participants describing sharing humorous, awe-inspiring, or otherwise memorable moments with friends or neighbors. For example, P2 described accessing the live video feed of his backyard to show his garden jalapeño plants to his friends. P8 recounted how she uploaded footage where her smart camera captured a bear in her neighborhood to YouTube, and also shared a humorous "highlights reel" of her son sleepwalking with other family members (which they later submitted to America's Funniest Home Videos). In other cases, participants described sharing videos with more serious evidentiary or disciplinary aims, as when P11 captured his friend's daughter getting into a fight on his smart camera, and shared it with his friend, the daughter's parent.

Video requests. In a few cases participants received requests from neighbors to review their camera data and send them any relevant recordings. P8's neighbors requested her SHC footage of a bear rummaging through the trash, which "helped debug what was happening." P8 further explained that her neighbors will rely on her and her smart camera as the neighborhood "point person": "They'll text me, 'Hey, can you see if this got caught on there?' . . . [and I respond], 'Maybe you should get these cameras."'

5.2.4 Smart Home Cameras as Device Actuation Systems. ***Control and actuation*** of other devices or systems is the final basic SHC capabilities we report. The most common example is configuring SHCs to deliver text or email notifications, or to automatically record video/audio. In common instances where users configured their cameras to send smartphone alerts that notify them when motion, sound, people, or familiar or unfamiliar faces are detected (P2, P3, P7, P8), SHC interfaces typically refer to these notifications as "events" or "moments," and enable users to configure their devices to automatically save events or moments to the cloud for retrospective review and documentation. However, these capabilities often require upgrading to paid subscriptions. The only other example of device actuation that we identified from our interviews was the use of SHCs to control external lights to deter potential thieves or intruders (P2). No participants reported availing themselves of features that enable control of built-in sirens or add-on smart power outlets.

5.3 Clear Limitations and Subtle Effects of Current Smart Home Camera Products

Participants also noted several prominent limitations to their uses of the SHCs and the types of extended sensory perception discussed above. Commonly cited pragmatic limitations include:

- **Lack of robust recording or storage access.** Paid upgraded subscriptions typically expunge video recordings after 30 days, thus requiring that the user manually downloads relevant video clips within this period. Without a paid subscription, recording capabilities are even more limited.
- **Irrelevant, inaccurate, and excessive smart alert notifications.** Many participants described motion, person, object, sound, and face alerts that were inaccurate or irrelevant. In some cases, participants consequently disabled notifications or became desensitized to them.
- **Practical obstacles to physically mounting, positioning, powering, and connecting the device.** Participants described difficulties positioning, repositioning, and installing devices because of the effort and skill required to mount the devices to walls or ceilings and physically connect them to a power source (currently, very few SHC products are battery powered). Participants also described limited Wi-Fi coverage as a major obstacle at times, especially when installing outdoor SHCs away from home routers.
- **Significant lag times when viewing live video/audio and receiving smart alert notifications,** which at times prevented users from monitoring or recording pertinent events. For example, alerts typically lag events by at least several seconds.
- **Difficulty achieving the right balance and targeting of device visibility/invisibility to others**, especially with minimizing visibility of the devices for neighbors and passersby while maximizing visibility to potential intruders.

Later in the discussion section, we observe that these limitations represent clear opportunities to improve the user experience of SHCs for primary users. Meanwhile, we however observe more subtly that some of these limitations *enhance* privacy and security for non-primary users and thus also represent latent privacy controls and safeguards.

We conclude this section by noting several seemingly unintended side-effects of the extended sensory perception enabled by smart home cameras. **(1) Avoiding camera fields.** A few participants described how they consciously avoid the SHC's surveillant field of view. P3 walks to another block to say goodbye to friends or "people of the opposite gender," as she is worried that her mother might watch or listen in on her with their SHC. P6, a food delivery driver, described parking away from cameras. **(2) Subtle pressure/intrusion of surveillance.** While this was reported in only a few cases (P6, P11), P11 memorably described feeling "subtle pressure" that caused him to be on his best behavior by, for example, not playing video games and staying productive at work. He explained that this pressure was partly based on knowledge that his mother-in-law—who lives with him and shares access to the SHC app—may be watching him. Interestingly, P11 describes reflecting on this "subtle pressure" only after he stopped using cameras during a move to another residence. Similar findings are reported by Pierce et al. [102]. **(3) Acclimating to smart cameras.** As participants introduced cameras into their home, some reported becoming acclimated to their use over time. P9 expressed that his "cameras are now like ornaments," indicating that the novelty of playing around with the smart camera's features wore off and that he now rarely directly engages his outdoor camera. Other participants, who lived with as many as one to ten indoor cameras, expressed no significant concerns about their privacy and security when asked. Our study suggests that some sizable portion of SHC users readily accept and rarely notice the near-constant surveillant gaze of cameras in their living rooms, entryways, kitchens, yards, and even bedrooms.

6 EVERYDAY SURVEILLANCE: FROM FORMAL OBSERVATION TO CASUAL PEEKING

In the previous section, we reported how participants used SHCs to extend sensory perception, deter undesirable behavior, communicate with others, document evidence, capture memories, and control other smart devices to support everyday activities. We now extend those findings by characterizing such uses as forms of surveillance. We loosely define surveillance in the more general sense of "the collection and storage of information, presumed to be useful, about people or objects" [37]. Yet we also intend the term surveillance to be read, at times, with the power-laden and potentially negative connotations associated with mass surveillance, carceral surveillance, spying, stalking, and so on. As our participants and scholars alike observe, surveillance—like any technology—is neither inherently good nor bad, but neither is it neutral [78]. As Rule states, surveillance "ranges from the benign to the repressive—from the personal information systems supporting intensive care in hospitals to those mobilized to track and curtail terrorists" [106].

This section examines *how* smart cameras mediate multiple modes of *everyday surveillance,* a term we use in reference to any broadly surveillant use enabled by commonplace and accessible consumer products and services within everyday contexts. We further find that these various surveillant uses occur along a spectrum from formal to casual surveillance, such as formally monitoring the home to deter intruders, to casually emergent forms of opportunistic, accidental, curiosity-driven, or one-off acts of surveillance. This spectrum is defined by three dimensions: *premeditation*, *focus*, and *regularity*. ***Formal surveillance*** is premeditated, it is focused with a specific aim or outcome, and it is often practiced on a regular basis. ***Casual surveillance***, on the other hand, is some combination of unplanned, unfocused, or irregular, such as overhearing a neighbor's conversation.

Adding to insights from surveillance studies, our research—albeit based on a small sample of committed SHC users—contributes further empirical evidence to the idea that surveillance is becoming a more accepted and even normative mode of everyday life, one which supports a much wider variety of activities than deterring, identifying, and punishing illegal or improper behavior. This includes surveillance as a mode of caring for others [72, 117], managing labor [117], feeding obsession and paranoia [70], maximizing monetary and social capital [26, 138], and tracking and regulating one's self [56, 83].

We organize our findings into six prominent types of surveillant uses of SHCs we identify: deterrent and regulating surveillance, managerial surveillance, care-based surveillance, diagnostic surveillance, cuing surveillance, and aesthetic and atelic surveillance.

6.1 Deterrent and Regulating Surveillance

Deterrent surveillance refers to instances where the threat of surveillance is used—often, we find, in a formal, premeditated manner—to deter behavior, particularly harmful, destructive, or invasive behavior such as theft, trespassing, and violence. More general than deterrent surveillance, regulating surveillance refers to uses that prompt or encourage the surveilled subject to self-regulate their own behavior. For example, P11 described an emergent use of constant SHC surveillance to regulate his nephew and children's behavior wherein he developed a habit of saying "let's check the cameras" when he suspected they may be lying. Both concepts of deterrent and regulatory surveillance are common concepts in surveillance literature (e.g., Foucault's disciplinary surveillance [46], Deleuze's control society [39]).

All participants indicated that deterrent surveillance was an important, if not sole motivation for installing SHCs and many suggested that their camera's core function was to provide security or safety. Yet, over time, some participants also discovered emergent and more casual forms of deterrent surveillance. Many such cases deterred relatively minor or petty offenses, rather than egregious or deleterious behavior such as burglary or home invasion. For example, P3 relayed that her mother noticed that neighbors stopped letting their "dogs poop in our yard" after installing the Nest camera, presumably because the dog owners noticed the camera. The above example is a rare occurrence in which a participant referenced material evidence to confirm the effectiveness of deterrent surveillance. As a basic observation, there is an inherent difficulty in verifying, on a case-by-case basis, to what extent SHCs deter rare or uncommon behaviors such as burglaries.

6.2 Managerial Surveillance

Participants described various surveillant uses of SHC aimed at managing and overseeing paid workers, particularly tradespeople such as carpenters, delivery workers, and domestic workers including nannies, babysitter, caregivers, and housekeepers. Our naming of this term is informed by Stark and Levy's notion of the "consumer as manager" [117]. Through analysis of contemporary smartphone applications, Stark and Levy argue that the "managerial logics of surveillance are proliferating across the digitally mediated service sector, enlisting customers as both managers and cheerleaders for workers themselves pressured by systematic and metricized expectations also out of their control." Our findings appear to support this broader cultural trend. However, our study focuses on how and why primary users engage in managerial surveillance—mediated through SHC extended sensory perception—and in some instances, offers a counter-perspective that highlights the value of managerial surveillance to the "consumer as manager."

For example, one participant (P4) explains how she uses her cameras to monitor her daughter's caretakers in case she is mistreated, as well as if "anything goes missing." For her, SHCs provide "an extra layer of protection." This suggests how the consumer as manager may surveil workers casually, and via the mode of *mere-potential monitoring and review* that we articulated previously. P12 describes going beyond mere-potential monitoring and review to engage in *direct anticipatory, focal, and retrospective monitoring and review* of her housekeeper and nanny to "check" to see if the nanny is "getting along" with her children: "If there are no cameras, you don't know what kind of behavior [they are] having around my kids." Interestingly, while P12 does bring up disputes to the nanny about situations she saw on camera, she does so indirectly without revealing that she was monitoring or reviewing the video footage from her SHC. She explains that doing so would be "detrimental" to their working relationship.

6.3 Care-based Surveillance

Participants described other instances where they surveilled loved ones to better care for them, or as an outward expression of their care. Stark and Levy refer to this role more generally as the "consumer as observer," through which surveillant products are used to supervise "intimate relations as a component of a normalized duty of care" [117]. Our notion of *care-based surveillance* aligns even closer with Alan Jacobs' observation that "[digitally mediated] surveillance has become the normative form of care" within our society [72].

Care-based surveillance of loved ones usually occurred while the participant was away from their home at work or traveling out of town. Two commonly cited examples were checking on kids and pets. For example, we previously discussed how P8 created a peripheral virtual window display to watch over her child playing outside in the cul-de-sac while she worked from her home office upstairs. In another example, P2 installed an indoor SHC to check on his puppy while away at work. While participants at times suggested that checking on pets was a form of anticipatory monitoring ("to keep an eye on the dog," in P2's case), they also described such monitoring as motivated by a desire to emotionally connect with pets when they are physically separated.

6.4 Diagnostic and Evidentiary Surveillance

Diagnostic surveillance refers to the use of surveillant technologies to diagnose the cause or effect of an event. *Evidentiary surveillance* was often suggested in conjunction with deterrent, managerial, and care-based uses—such as helping identify an unsuccessfully deterred intruder or confronting a negligent caretaker. Here we present three brief sets of examples, which range from formal and serious to casual and playful.

Evidencing crimes. Participants described a few instances where they provided local police with smart camera footage as evidence. P11 recounted a traumatic break in experience in which SHC footage helped them discover how the intruder had entered their home. P10 also discussed various instances where she used her smart camera footage to identify and provide evidence to the police, such as a hit-and-run of a parked car, stolen bikes, an assault, and various harassment issues in the neighborhood.

Settling disputes. In several cases, participants used SHC data to help settle family or neighborhood disputes. Participants described reviewing their smart camera footage to discover evidence when their kids fought with the family pet (P8) or with each other (P11), and settling crime disputes related to theft and harassment from neighbors (P10).

Reviewing remarkable, entertaining, or unexplained events. In contrast to the relatively high stakes disputes above, participants contrastingly presented many examples of fun, amusing, and sometimes sensational diagnostics and evidentiary SHC video. Examples include retrospectively reviewing their video history to find footage of a bear eating from their trash cans (P8), a video of an approaching tornado (P4), and a video of a family member being followed by their chickens (P11).

6.5 Cuing Surveillance

Cuing surveillance refers to when people use surveillance to anticipatorily notify them of events that may require specific action. This type of surveillance involves the mode of anticipatory monitoring we discussed previously and is often enabled by smart alerts to detect motion, people, or familiar or unfamiliar faces. The doorway was the most common site in which participants described formally and regularly using cuing surveillance. Examples of cuing surveillance include (1) knowing when an expected guest has arrived, as a cue to answer the door and sometimes to finish readying the home by, for example, kenneling dogs or putting kids to sleep (e.g., P3, P7, P8, P14); (2) knowing when someone is at the door, as a cue to see who's there and decide whether and how to answer (e.g., P3, P4, P13); and (3) knowing when a package has arrived, as a cue to take it in or sometimes to thank or confirm to the deliverer that it was received (e.g., P4, P7, P8, P13). Some participants also mentioned surveilling disabled or older family members and kids, as a cue to help them if they fall or need assistance (e.g., P1, P4).

A few participants described comparatively unique types of cuing surveillance that they regularly engaged in. For example, P4 uses a doorbell camera to know precisely when her daughter's special medicine arrives, to ensure she refrigerates it before it spoils. These examples suggest how future smart cameras and sensing systems might enable even more personalized, ad-hoc, idiosyncratic modes of everyday surveillance.

6.6 Aesthetic and Atelic Surveillance

The surveillant use categories described thus far are usually directed toward a relatively clear aim or outcome. Yet we also uncovered instances where SHC surveillance was discussed as predominantly or partially motivated by more emergent and less instrumental drives associated with curiosity, excitement, entertainment, reminiscence, and other experiences. We characterize such uses as a combination of aesthetic and atelic surveillance. *Aesthetic surveillance* occurs when users are inspired to sensuously engage with surveillant information because it is pleasing, intriguing, beautiful, shocking, and so on. *Atelic surveillance* occurs when users apply surveillance technologies without a clear instrumental purpose or outcome, but rather a sense of emergent, momentary, or open-ended engagement. We describe several more specific variations below.

Surveillant noticing. At a basic sensory level, aesthetic and atelic surveillance sometimes appear to begin as merely a modified form of everyday noticing akin to looking out the window or overhearing a conversation. For example, P13 recalls a time her SHC enabled her to watch various events or commotion on her street, citing small neighborhood parades to celebrate essential workers during the COVID-19 pandemic, "couples having arguments," or a bike being stolen. She explains, "If you catch it at interesting times, it's New York City, you'll always see something kind of like crazy." However, in many other cases, such acts of noticing would have been difficult if not impossible without the extended sensory perception of the SHC, such as remote viewing, recorded timeline histories, and smart alerts. Furthermore, the capabilities and affordances of the SHC system often shield the viewer from being observed by a surveilled subject.

Curiosity-driven surveillance. Several participants described casually observing behaviors and overhearing conversations of neighbors, passersby, friends, or even themselves. P3 describes occasional situations where the SHC prompts her to casually watch

neighbors and passersby: "Sometimes if I stay up super late, I'll get notifications on my phone about motion detection, and I'll go, 'What the hell are people doing at 4AM or 12AM at night?' People are jogging! And if I'm up and I just want to see what's going on, sometimes I'll listen in on neighbors' conversations." P13 talked about hearing her neighbors' arguments, slamming doors, seeing who might be storming out of the building "not to be nosy, but I guess also to be nosy."

Reflexive surveillance. Surveillant noticing also led to deeper reflection on the interplay between one's surveillant smart camera and environment. P8, for example, described how the smart recognition capability of her doorbell camera regularly mistook her friend's husband for her own husband because they dress similarly. P8 later shared this information with her friends in a humorous manner, and her husband at one point even attempted at one point to dress up as their friend to "spoof" the camera. This example illustrates how a surveillant noticing led to insight both about her own life and the inner workings of the camera.

Surveillant memory-making. Some participants described premeditated use of their smart home cameras in ways that closely approximated the typical usage of smartphone cameras or action cameras (such as a GoPro) to capture meaningful moments in their lives. For example, P10 owns a Wyze camera that she moves to different places to monitor her kids throughout the house. P10 further reflected on an instance in which she set up this camera specifically to document a Christmas scavenger hunt she had designed for her children. Participants also suggested a more novel form of video photography in which meaningful moments are inadvertently or unexpectedly caught on camera. In addition to examples of natural disasters and animal spotting previously reported, other examples include saving funny or memorable moments of P11's cat getting scared on camera, performing Brazilian jiu jitsu, and videos of his daughters calling each other funny names. These uses parallel use cases depicted in SHC marketing materials, such as Nest advertisements which suggest cameras can be used to record a baby's first steps, for instance.

Self-reflective and self-conscious surveillance. In a few instances, participants described retrospectively reviewing video and audio of themselves and their interactions with others. P3 described times when she reviews video of herself with friends to "just to see what happened," "to see how the interaction went," and "to see how I look and stuff like that."

7 TWO AXES OF ASYMMETRY FOR ANALYZING PRIVACY, SECURITY, TRUST, AND POWER

In this final section of findings, we dig deeper into perceptual and power asymmetries with the smart camera, and their connection to data privacy, security, and trust. We divide our reporting and analysis into two sections, each representing an axis of asymmetry: frontend users and backend users, and primary users and non-primary users.

7.1 Frontend and Backend Users

Studies of user privacy and security often focus on how companies or malicious actors might use people's personal data. Here, we refine this notion by distinguishing between frontend users who own, install, and operate SHCs, versus companies, platforms, service providers, and other backend actors, notably malicious actors like hackers and cyberstalkers. A *backend user* is one who accesses a system and its data such that the frontend user is oblivious to or only peripherally aware of the backend user and their uses. Typically the backend user interfaces with this data via network connection, rather than, say, physical theft of a device. A prime example is a smart device company that accesses, shares, and utilizes frontend users' SHC data for reasons other than or in addition to directly providing feedback or value to those frontend users. Reciprocally, a *frontend user* is any user oblivious or only tangentially aware of backend users and their uses of the data. While a backend user is not necessarily nefarious or malicious, backend uses do often dovetail with Zuboff's concept of "surveillance capitalism" [138], and the related concept of "hole-and-corner applications" [101] that are hidden from and potentially harmful to frontend users.

Below we describe our participants' awareness, attitudes, and practical orientations toward their own privacy, and toward backend users, specifically three main groups that repeatedly surface during our interviews: (1) companies, manufacturers, platforms, service providers, and "third parties", (2) hackers, cybercriminals, and other malicious actors, and (3) state and foreign authorities, including perceptions of interference by international governments and local police.

7.1.1 Steps Taken to Increase Privacy, Security, Trust, and Control.

While most primary users did not express much concern about their own data privacy and security regarding their SHCs, there were some exceptions. Some brought up concerns that "China" might have access to their data (P2, P11, P9). Others indicated differences in trust among brands to safeguard their personal data. P2, for example, mentioned how he did not trust Wyze because they are a Chinese company, and was wary of how cheap Wyze devices were: "It almost seems too good to be true. . . someone's gotta be subsidizing the data or something."[1] To P2, "if it's free or cheap, you are the product." P8, in contrast, mentioned that she and her husband are early Wyze Cam adopters, and wanted to support the brand because they are headquartered locally. Two participants expressed suspicion with Amazon and were wary of them using their SHC data for marketing purposes (P9, P11). P13 reflected that she "probably should" be more concerned about her data on the smart camera.

Some participants did, however, take sophisticated technical steps to protect their privacy and security. One salient example was P11, who customized his camera system (which connects to his 25 smart home cameras) to operate only locally through a combination of local SD card device storage and use of a custom app for managing their SHC data. Others decided to stop using devices. Out of concern about Wyze's ability to record and save 24/7 footage inside his home

[1]Note that, according to the Wyze website they are a US company based in a major US city. We recognize that these claims may fall into potentially harmful and incorrect cultural, political, and xenophobic political assumptions or stereotypes, though we include this finding to represent participants' experiences of mistrust. While participants' comments suggest that this mistrust may be influenced by a variety of factors (such as news reporting, exposure to online information, political beliefs, or other experiences), we do not have enough data to analyze the root causes of these statements and beliefs in this paper.

(coupled with concerns already listed), P2 uninstalled the camera after spending more time with it while working from home.

The placement and installation of their cameras was the one notable area in which *all* participants expressed some level of distrust and concern for their privacy and security, and many participants highlighted areas where they disallowed SHCs. For example, P7 and P9 were adamant that they would be uncomfortable with *any* indoor cameras. On the other hand, P4 and P8—who each live with multiple indoor smart cameras that are virtually always monitoring—expressed that their bathrooms and bedrooms were non-negotiable "off limits" areas for SHCs, but that anywhere else is fine. Similar to variance in how users manage boundaries with online privacy (e.g., [3]), these findings suggest that there is also variance with how primary users conceptualize and manage boundaries with respect to SHCs and IoT sensing devices more generally. This finding is echoed in Chalhoub et al.'s longitudinal study of smart home products, where participants expressed varied and changing perspectives about their comfort level with microphone and camera enabled devices in areas such as bathrooms and bedrooms [29].

7.1.2 High Trust and Low Concern with Backend Users and Personal Privacy and Security. Participants had much to say about the various (frontend) uses of their SHCs but had comparatively less to say about backend users/uses and their personal data privacy and security. Only towards the later portion of our interview did we explicitly ask participants about privacy, security, and trust with respect to companies, hackers, and other backend users and uses of their data. Participants mostly expressed little concern for their own personal data privacy and security, though we discuss some notable exceptions further below. While participants noted various technical shortcomings of the cameras—including connectivity issues, video lag of seconds or minutes, and inaccurate or irrelevant notifications—participants rarely expressed distrust in the device manufacturers and service providers.

When asked about potential privacy or security concerns, our analysis of participant responses surfaced 6 types of reactions that may explain why they expressed little concern with privacy and security. We encapsulate each general reaction in first-person terms, and briefly exemplify each. ***(1) I have little to hide.*** When asked about data privacy, P8 and her husband indicated they were "pretty boring" people and had "nothing to hide from" one another. ***(2) The risk is very low.*** P1 described his chances of getting "hacked" as low, "because I'm not a high-profile person." ***(3) The benefits outweigh any risks.*** P1, continuing from above, went on to say that he sees SHCs "as more helpful than the chance of getting hacked for something." P4 responded to our questions about privacy by stating, "if I have to worry about [privacy], then I shouldn't have a camera", and described the importance of monitoring her caregivers to ensure they were properly caring for her family. P3 explained how her SHC use was motivated by a lack of trust in the police to protect her security and safety, stating that her Nest camera was more effective and trustworthy than local police. ***(4) I have sufficient control.*** P8 responded to our questions about privacy by emphasizing that none of her indoor cameras—even the active camera in her bedroom—are pointed *at* the bed to avoid capturing anything "intimate": "As long as they're not pointed at the bed, we're not concerned." ***(5) I hadn't thought of that.*** When asked about privacy concerns regarding their data (P13) and consideration for their neighbors' privacy (P7), both responded that maybe they should be more conscious of this. ***(6) I only see what's in front of me.*** While no participants directly stated that they did not consider or concern themselves with backend privacy and security threats because these threats remained out of sight, this explanation is suggested in the preceding examples—namely that participants had much to say about their firsthand uses of their SHCs but had little to say about actual or potential backend uses by companies, criminals, or governments. Furthermore, many participants demonstrated insufficient or inaccurate technical knowledge about their SHCs and potential privacy and security implications, which we discuss further below.

7.1.3 Limited Knowledge of Backend Uses and Implications for Privacy and Security. Consistent with Zheng et al.'s findings [137], participants in our study sometimes demonstrated incomplete or incorrect knowledge of backend and future system capabilities. Here we present one instance that exemplifies how imprecise mental models may be formed from interface features directly available to the user (frontend capabilities), without considering how a company may independently access, store, analyze, and share user data (backend capabilities). P2 notes that Amazon Ring requires an upgraded paid subscription to record videos and save them to the cloud, and uses this to infer how Amazon is handling his data:

> "[Knowing that Amazon requires a paid subscription] is good for me because it means that it's not being recorded somewhere else. . . I mean, if they had the data being saved, I assumed that they would just give it to you for free as, like, a service. But if you're not paying them, they're probably just not recording anything." —P2

Here, P2 reasons that what he sees on his smartphone interface mirrors any backend processing that might be "recorded somewhere else": While we cannot know with certainty to what extent P2's SHC device data (and metadata) are in fact being stored and analyzed by Amazon, this example illustrates the temptation to infer that backend capabilities are limited to the frontend interfaces one can see and use—even though this technically is often not the case.

Following Kahneman's concept of the WYSIATI bias (What You See Is All There Is) [74], we refocus this idea to hypothesize a specific bias about digital user interfaces, especially with cloud computing applications: *WYSOYIATI—What You See On Your Interface Is All There Is.* The correct mental model, however, is *WYSIJYI—What You See Is Just Your Interface.* Which is to say, your user interface application is just *your* (frontend) interface (but there are also *backend* interfaces and applications).

7.2 Primary Users, Non-Primary Users, and Interpersonal Power Asymmetries

Next, we focus on the second prominent power differential: the relationship between primary users and non-primary users. In the context of our study, ***primary users*** are those own, install, and operate consumer SHC products. ***Non-primary users*** are those who, at some level, interact with SHCs but do so with comparatively limited access, control, feedback, consent, awareness, or benefit,

and often with increased associated risk or harm. This notion of a non-primary is more general than a bystander, in that it captures situations where someone with partial consent or awareness of device's presence interacts with it (e.g. a worker delivering a package, or a friend visiting and noticing a camera is present). The concept of a non-primary user addresses situations where a subject is not an innocent or accidental bystander, but rather an intended subject of surveillance. In some scenarios, SHCs sense or surveil completely unaware and non-consenting subjects, in which we follow Baumer [11] and may qualify such subjects as ***usees***, rather than ***users***. For simplicity, in this paper we often refer to non-primary users and usees collectively as non-primary users. (Note that the primary users and non-primary we reference are both frontend users with respect to the backend actors we discussed previously—companies, cybercriminals, and government actors.)

While our participant sample gives us a limited vantage point onto many important non-primary user perspectives—including those of nannies, housekeepers, guests, and passersby—our study does, by design, provide three routes to understanding non-primary users and uses. First, we present findings related to how primary users do and do not consider non-primary users. Second, nearly all our primary user participants also describe events where they occupied a role as a non-primary user, either with respect to their own SHCs or those managed by others. Third, two participants in our study worked in prominent non-primary user roles affected by SHCs: a delivery driver and census worker.

7.2.1 Limited Concern for Privacy and Security of Non-Primary Users. Most primary users we talked to had limited concern for non-primary users' privacy. Here, we present several typified and example responses to our questions concerning non-primary users' privacy and security.

(1) It's my home and my safety. P1 rationalizes that recording others is acceptable and that he does not have to explain to guests that they have a home camera. "I'm not using it for commercial purposes, it's for my personal security and I would be getting some sort of consent just in case I needed to publish it publicly . . . It's my house." P3 echoes this sentiment, further adding that her neighbors and passersby know she has a camera—presumably because they can see it—but "it's whatever . . . you can't just tell someone to take their stuff down so people don't say anything." ***(2) It's legal.*** Several participants referenced laws around recording and consent. P9 explained that she does not have privacy if police want to investigate a crime using her Ring camera. P9 also explains that while in "public" she does not have privacy because she lives in a one-party recording state (i.e., other parties do not have to have consent for recording in public). ***(3) It's expected.*** Several participants expressed that people should expect to be recorded in public these days. P2 stated: "It's 2021 . . . so I'm not going to immediately jump to be like, 'Oh, let me cover the camera up.' If we're all just sitting on the porch, hanging out, I don't think any of my friends would mind." ***(4) They don't mind.*** When asked about their family's, neighbors', and domestic workers' orientations to their SHCs, many primary users explained that specific non-primary users, like their kids or parents, found the devices acceptable or useful, or hardly noticed them. P9 said that her kids are of a generation where they grow up with cameras everywhere and are used to being recorded. P1 explained that his older parents do not understand how the camera works because it is "techy," but they trust that the camera is useful. ***(5) I can relate.*** In some instances, including several described above, participants described themselves in a general role as a non-primary user (e.g., "It's 2021" and referencing one-party consent state laws) to explain why they do not mind, or why they do not expect personal privacy.

(6) They're protected / I'm using it responsibly. In contrast to the above explanations, in some cases participants described how they did not dwell on non-primary users' privacy because the way they configured or used the devices tacitly protected them. For example, P3 explains that being able to see her neighbor's house and sometimes overhearing their conversations through her Nest camera is okay because the SHC is not recording—"as soon as they [the neighbors and their conversations] leave, it's gone in my head because I'm not recording anything."

7.2.2 Positive Considerations for Privacy and Security of Non-Primary Users. In contrast to the above responses, some participants expressed forward-looking concern for non-primary users and took concrete steps to protect their privacy. For example, P9 uses activity zones in his Ring camera to avoid recording areas pertaining to his neighbor's yard and to avoid getting motion alerts for those areas. P2's neighbor's privacy was also a consideration for him regarding his camera placement, as P2 had removed his Ring camera from his front door when he realized that it also captured a full view of his neighbor's door across from him. P10 alerted her neighbors that she had a camera when she installed it, and P9 asked his neighbors if they were okay with him setting up a SHC.

Regarding indoor SHCs, P11 explained that he was very conscious when a guest was staying over. To protect their guest's privacy and communicate that his devices were deactivated, he unplugged his SHC and positioned it facing down. P11 further explained that he took this secure and subtly visible action preemptively, *without* asking guests if they mind the cameras, to avoid imparting any pressure for them to consent.

7.2.3 Perspectives as and on Non-Primary Users. Our study included two participants who worked in occupations in which they regularly interacted with SHCs as non-primary users. Within this limited sample we nonetheless see differing perspectives. P7, a census taker, had little to say about her interaction with SHCs other than that they were common, but that the Ring doorbell communication features were often technically faulty. P7 implied this was a shortcoming that prevented the devices from helping her do her job.

P6, a young woman who works as a delivery driver and is within presumed sight of her neighbors' smart cameras, had much more to say from these perspectives. To her, smart cameras take away people's "last shred of privacy" and create a "breach of privacy to other people because it's not selective on who it's filming." At a more personal level, P6 says, "I don't like being on someone's camera that I don't even know. You never know what they're doing with the film," and is concerned people are using cameras for "voyeuristic" activities. P6 also describes steps she takes to avoid being recorded on SHCs in her work as a delivery driver:

> "If I notice that the house has a Ring camera, I will purposely drive past the view of the Ring camera

> before I get out and drop the food off. Or, if I notice that they have a camera in their driveway pointing a different direction, I will park behind wherever it's pointing to stay out of the frame. I do kind of avoid it a little bit and again, [but] it's not like I'm doing anything that I'm afraid to be seen. It's just, I guess it's my fight to still maintain [my anonymity], you know?" —P6

However, P6 also acknowledged the need and right for people to protect their privacy, and that the police should be able to access cameras if they are "doing bad stuff." Several primary users also relayed experiences where they found themselves in the position of non-primary as a guest or visitor. For example, P9 expressed criticism of how some of his family used SHCs. P9, who only has outdoor SHCs, disapproved of his sister's use of indoor cameras. He described several specific incidents where he visited his sister and felt uncomfortable with use of the cameras to surveil both his family and her own family, and suggested his sister did not need this degree of surveillance in her "gated community."

P10 talked about how she tends to stay away from the Ring Neighbors app and other platforms such as Nextdoor or certain Facebook groups where people regularly post and request smart camera videos of incidents. She avoids these platforms because she finds their content racially targeted: "it seemed like everybody that you caught on video and posted was Black or a person of color." She reflected on her identity as a Mexican woman and it seemed to her that people would just post any suspicious activity, unsubstantiated activity of a Black person—such as simply walking across someone's yard. These experiences are best summed in P10's statement: "Either the people that utilize them are racist and they don't know it, or racist and they won't admit it."

8 DISCUSSION

Based on our findings, we elaborate upon four key insights that emerge from our analysis and reporting.

1. People use smart home cameras as multi-functional technologies. The narrow product marketing nomenclature of "smart home security camera," which implies a straightforward extension of older home security cameras, belies the diverse range of SHC uses we uncovered. Our work suggests that researchers and designers should understand smart home security cameras as more than image-capturing cameras, and more than conventional home security devices for deterring and protecting against intruders or thieves. Our empirical findings, in conversation with prior critical writing [101], lead us to conceptualize these devices as *extended sensory perception technologies*. In turn, we found these sensory-perceptual capabilities supported behavioral deterrence, communication, documentation, and the control and actuation of other systems.

Beyond conventional home security and safety applications, we found participants used SHCs as multi-functional technologies to support a variety of everyday activities—from managing guests and packages, to checking on pets and kids, to casually spying on neighbors out of curiosity. In some cases, participant uses of SHCs align with various "third-wave HCI" [19] concerns including aesthetic engagement, reminiscence [95], reflection [10, 110], creativity [126], and social connection. We thus extend and specify related work with IoT systems (including the smart camera) on how users reappropriate such devices for pleasure [118] or entertainment [29] by identifying these categories of adoption through multiple forms of monitoring.

2. Smart home cameras are spatially sensitive and perceptually powerful devices. The landscape of interactive, networked-connected, sensor-enabled, and data-driven devices is vast and expanding. Through identifying many forms of monitoring in smart home cameras, our study highlights the need to distinguish an important subset of smart devices that hold unique and significant implications for user privacy, security, trust, and power: *spatially sensitive and perceptually powerful* smart devices. In contrast to *personal* computing devices and applications such as laptop web-browsers or smartwatch heart rate monitoring, SHCs are spatially sensitive devices in that their capacity to digitally detect data physically extends within large areas of the private home, and across long distances of space. But whereas an isolated heartrate sensor or temperature sensor offers only a narrow range of sensory-perceptual power, smart home cameras enable a much broader and deeper array of information and insight. Underpinned by cloud and edge computing—and enhanced by computer vision, far-field voice recognition, and other machine learning techniques—current SHC systems are capable of motion detection, noise detection, person detection, object detection, facial recognition, and "unusual activity" detection. In the future, new and emergent inference and prediction capabilities will likely become more robust, accessible, and mainstream—such as more advanced emotion or facial recognition mechanisms.

3. Smart home cameras invariably involve non-primary users. A key insight of our study, confirmed and nuanced by our findings, is that in practice SHCs invariably affect non-primary users' experiences and practices, and their privacy and security. We further find the non-primary users often *interact* with smart home cameras, at least from the perspective of primary users. This non-primary user and usee interaction with SHCs typically involves very little awareness, consent, access, control, feedback, and benefit—key qualities that typically define a *user* experience. We found that non-primary users/usee interactions with SHCs was extremely common, and ranged from surveilling kids and family with implied or tacit consent and awareness (secondary users), delivery drivers and guests (indirect or incidental users [80, 137]), domestic workers with borderline consent and awareness (partially-consenting users), and neighbors and passersby with little or no apparent awareness or consent (non-consenting usees [11]). More work is needed to further characterize the various valences here, including bystander [133], incidental user [80, 137], usee [11], and non-user [12, 108] perspectives with respect to spatially sensitive and perceptually powerful smart devices.

Understanding these actors *as users*, rather than mere subjects or stakeholders, underscores our finding that in many cases non-primary users appear to have some significant degree of awareness of the presence, capabilities, and effects of interaction with the SHC, as well as some minimal degree of consent, albeit tacit or coerced. An illustrative example is the case of delivery driver or guest who typically notices a smart camera in the doorway or entryway, understands at least some of its capabilities, and then drops off a package

or decides whether to ring the doorbell with awareness that they are interacting with a smart sensing technology that may well be alerting and displaying their activity to the resident. Our study surfaces mundane yet illuminating examples of such interactions, ranging from neighbors who wait patiently without knocking to be greeted at the door (P8) to delivery drivers who seek to avoid the surveillant gaze of smart cameras by parking further down the street (P6). We further saw concretely how the spatial sensitivity of smart home cameras (and built-in microphones) enables users to surveil neighbors and passersby through windows, across streets, and over property lines. Another benefit of conceptualizing these subjects as users, rather than merely surveilled subjects, is that it helps encourage us to attend to them with the usual considerations we give to users—such as maximizing benefit, reducing harm, and creating a usable, useful, and enjoyable experience.

4. Smart home cameras support, enable, and invite formal, casual, and emergent surveillant uses. According to various strands of technological mediation theory (e.g., [45, 124, 125]), we shape technologies, and in turn, technologies shape us. Analyzing our findings through this theoretical lens, we argue that SHCs support and subsequently invite and encourage emergent surveillant uses. This happens in many ways, including pushing surveillant notifications in front of users' attention, and bringing surveillant access to their fingertips at the press of a smartphone button. Our findings demonstrate a multitude of ways that primary users engage in SHC-mediated surveillance of non-primary users and other subjects for a variety of purposes—including behavioral deterrence, managing workers, caring for loved ones, cuing specific actions, and comparatively aimless, open-ended aesthetic and atelic engagements. This paper further has drawn connections between these findings and concepts from surveillance studies, including Stark and Levy's surveillant consumer [117], Zuboff's surveillance capitalism [138] and foundational concepts from surveillance studies, such as regulatory or disciplinary surveillance [39, 46, 50].

9 DESIGN INSIGHTS AND OPPORTUNITIES FOR ADDRESSING PRIVACY, SECURITY, AND POWER

We conclude by outlining design insights and opportunities for improving smart home cameras, particularly addressing privacy, security, and trust regarding both primary and non-primary users, and frontend and backend users. From the perspective of primary SHC users, we found that while these devices were often highly valued, they nonetheless possess some significant technical and practical limitations. From the perspective of non-primary users and usees, we have identified an overall power imbalance with SHCs, along with specific security threats and privacy harms. Together these two findings leave us, as technology designers and researchers, in a difficult position—a position we hope our work clarifies, and impresses, upon the reader.

Turning toward solutions and responses to improve this situation, we find ourselves in a generalized design dilemma: how to support the needs and desires of primary users (and paying customer) in ways that are not invasive and harmful to non-primary users. While we argue that it is critical that designers better understand and address the effects of primary users' surveillance uses of non-primary users and usees, at the same time our research also identifies clear opportunities to improve and expand the capabilities and user experience of SHCs for (surveillant) primary users. Considering both sides of the primary/non-primary differential, we argue, is necessary to develop more effective and equitable systems, which in some cases may best be handled contextually [94] and locally [84]. We examine each side of the primary/non-primary user divide in turn, and then merge our two sets of insights to outline paths toward more effective and equitable designs.

9.1 Improving, Expanding, and Limiting Smart Cameras to Increase Privacy, Security, and Equity

While surveillance often appropriately carries a pejorative connotation, our findings also foreground surveillance applications that provided real benefits to our participants. These ranged from convenience in managing mundane practical affairs (e.g., kenneling the dog before answering the door), to connecting and sharing with others (e.g., checking on pets, capturing memories), caring for other family members, to deterring and documenting incidents of abuse and negligence from caretakers. Beyond the clear-cut areas for improvement noted in Section 5.3, participants at times demonstrated creative appropriations and workarounds that suggest opportunities for further enhancing and expanding the design of SHCs.

Mobile, ad-hoc cameras, and remotely repositionable cameras. While the design and marketing materials of SHCs suggest these devices are intended to be left in a relatively stationary position, several participants described regularly moving a SHC around their home to aid in various tasks such as keeping an eye on kids or pets. Two participants devised household names to refer cameras dedicated for mobile and ad hoc uses—"the spare camera" (P8) and "the nanny camera" (to imply P10's mobile use of the camera for care-based surveillance over her children) (P10). This suggests an opportunity to better support mobile smart home camera applications, perhaps through more adjustable fixtures, battery powered devices with inductive base chargers, or improved remote lens repositioning features offered by some SHC products.

Circumventing the cloud and backend uses. One participant, P11, described taking his smart home camera completely "off the cloud" because he did not trust presumed backend users (the manufacturer and "the Chinese government"). This and other uses suggest a need and opportunity to better enable SHC users to select or switch between cloud and local storage, while also clarify performance limitations of doing so.

Ambient and peripheral displays. We reported one noteworthy instance where a participant created a peripheral display to monitor her kids playing outside (P8). This and other uses suggest a need and opportunity to better support focal and peripheral monitoring, such as combing a more mobile SHC device with a similarly more mobile and adjustable dedicated display screen.

Targeted visibility/invisibility. Participants described challenges with achieving the desired outcome of conspicuously showcasing SHCs to potential intruders, while concealing or minimizing the visibility of the devices so as not to annoy or offend their neighbors. This presents a few opportunities for enhanced filtering

capabilities, though we note that such filtering may also enable more invasive and discriminatory targeting behaviors. For one, improved analytics capabilities may allow primary users to automatically filter different subjects—whether someone is distant, nearby, trespassing, or lingering—which would then allow users to adjust visibility parameters (i.e. the various intensities of indicator lights and alarms). These filters could also control physical mechanisms, such as the type of mechanical "privacy shutter" devised by Cheng et al [31]. Future work may also consider how filters can support non-primary users' privacy preferences. However, it is possible that some of the analytics required to identify the presence of non-primary users may be interpreted as privacy-invasive or overly surveillant. Secondary sensors, rather than image and video analytics, could also be used to implement these filters. To protect the privacy of neighbors and passersby, a SHC might remain visibly closed most of the time. However, if motion is detected on one's property at night, the camera "awakens" and the physical shutter detracts and lens opening illuminates. Such a technique is also sometimes employed in science fiction films to dramatically personify surveillance systems. More simply, a SHC system could enable a user to manually switch between different levels of visibility/invisibility.

9.2 Personal Controls for Personal Privacy

Primary users generally expressed high degrees of trust and control of their SHCs. None directly expressed desires for new or improved privacy or security controls, and few took significant steps to protect their privacy with SHCs outside of determining its location and position, and who should have access to the app interface. Many participants describe leaving cameras on most of the time, even in private settings like the living room or child's bedroom. One exception was P11 who undertook several steps to visually communicate to a guest that his SHCs were deactivated, by unplugging and positioning his SHC face down on the ground. This suggests a need and opportunity for more easily and visibly "closed" devices, to help assure guests and visitors that the devices are indeed disabled (c.f., [102]).

Overall, our research would seem to confirm Zheng et al.'s finding [137] that users generally trust smart devices (and backend users/uses), yet at the same time, these users often possess limited knowledge about the types and extent of insight that machine learning can infer about their lives. They propose that users might express greater concern about their privacy with greater awareness. However, assuming this motivates users to protect their privacy, it seems unlikely that some SHC companies would be incentivized to reveal their backend uses of SHC data. Thus, this suggests that tools to motivate or educate primary users about backend uses must continue to come from relatively independent designers, artists, activist groups, or governments—ranging from awareness campaigns, to op-eds, to art and design exhibitions [119].

9.3 Controls for Non-Primary User Privacy and Security

Primary User Side Controls. Perhaps the most obvious design approach for improving privacy for non-primary users/usees is to empower and nudge them to configure and operate their devices in ways that better protect non-primary users. Several participants took steps specifically to safeguard the privacy and security of non-primary users. For example, P9 used the "activity zone" feature to constrain the application of motion and person alerts to his own yard, and to exclude his neighbor's home. P3 described how using her camera without a subscription (so it only saves short snippets of videos) protects her neighbors' privacy, though she still listens in on small portions of their conversations.

On one hand, these examples suggest that new or foregrounded interface features could support and encourage primary users to help protect non-primary users' privacy and security by limiting overall sensing capabilities (e.g., not saving recordings) or discriminately sensing (e.g., specifying areas to exclude from recordings or notifications). On the other hand, these examples illustrate an inherent and serious limitation of primary user side controls: they remain invisible and unverifiable to any non-primary without access to the interface. Thus, while simple steps such as configuring exclusion zones and allowing recordings to be automatically deleted may in fact achieve suitable privacy for non-primary users, a neighbor or passersby has no way of knowing or verifying these settings just by looking at the smart camera. Even the indicator light and opening of the camera lens may be misleading, as many cameras possess wide-angle visual fields, and some allow users to dim the indicator light while it is actively sensing.

Non-Primary User Side Protections and Interventions. Another route is to empower non-primary users with tools to protect their own privacy. This approach is illustrated by techniques such as Truong et al.'s infrared LED camera sensor blocking device [122] and Chen et al.'s wearable ultrasonic microphone jamming technique [30]. It is also explored in Harvey's counter-facial-recognition makeup [65], Shepard's CCD-Me-Not Umbrella [112], and Pierce's CCD-Me-Not Curtains [101]—an open riff on Shepard's speculative design concept. More generally, we might design technologies that help the homeowner circumvent, say, a surveillant neighbor as much as an activist might circumvent surveillant states [107]. However, such tools have significant technical, practical, and legal limitations. For example, surveilled individuals rarely have practical and legal ways of accessing and controlling someone else's digital surveillance system. Hence, each of the counter-surveillance tools above is a standalone hardware or non-computational tool.

Shared or Negotiated Controls. A third design direction is to develop better shared and negotiated controls. Many devices already support access for trusted secondary users like spouses, children, or housemates. There are also examples of specialized portals for mediating the sharing of sensitive personal data, notably Ring's video request portal for formally requesting footage of serious incidents such as car accidents or abductions. However, neither of these features do much to address the effects of perceptually powerful and surveillant SHCs on neighbors, domestic workers, houseguests, and passersby. Despite significant legal, technical, and usability hurdles, one might imagine a *notice-and-contest portal*—like Ring's video request portal, but instead functioning as a mechanism for formally requesting that someone limit or disable a device pointed at their property or window. We might also imagine legal provisions that require SHC service providers to add ways for people to "opt out" of video feeds through dynamic masking to block their faces and bodies, or to notify individuals of devices

breaching their properties or bodies. These implications extend potential cooperative mechanisms for managing bystander privacy in other technologies, such as information and footage deletion request features for drone bystanders [134].

9.4 Latent and Embedded Controls and Safeguards

Common approaches to usable privacy and security typically rely upon notice and consent [114, 115], and individual user interface controls (e.g., [2]). A different approach we propose is to design *latent and embedded controls and safeguards*. Our study uncovered many instances where technical or practical limitations of the SHCs appeared to inadvertently create privacy protections. For example, many users described not paying for cloud subscription upgrades, which limited their ability to collect surveillant histories. Even when participants did upgrade, the systems do not typically store user accessible video or other data for longer than 30 days. This suggests a latent privacy safeguard that inhibits users from acquiring detailed, searchable databases. While it is technically possible to download all SHC camera data, in practice this is prohibitively cumbersome and is not readily supported by the app or platform. These findings parallel design directions from prior work analyzing the implications of ubiquitous digital trails for victims of state surveillance, in which researchers argue for enhancing plausible deniability in technologies—indicating a need to design systems for ephemerality, rather than permanence [107].

In addition to the disincentive of paying for cloud subscription as one latent privacy safeguard, our participants also discussed the mediating effects of the size and visibility of the camera's housing and form-factor, often desiring that it was visible enough to deter intruders but not so visible as to draw the ire or alarm of neighbors. This need to maintain balance (between being just visible enough, but not too visible), may inadvertently help protect the privacy of neighbors by alerting them to the presence of the devices. Further, while SHCs are lighter, cheaper, and easier to setup than older video surveillance cameras, participants still described cost and practical barriers to achieving more complete coverage of their property. These examples and other limitations suggest design opportunities to deliberately embed controls and safeguards that inhibit and discourage primary users from overly invasive (though often inadvertent) surveillance of non-primary users—though may fall short of outright preventing them from doing so.

9.5 Informing the Design of Laws, Regulations, and Policy

Finally, we would be remiss to neglect the relevance of policy and law to these issues—perspectives that are increasingly discussed within HCI (e.g., [116, 131]). Such policy interventions are necessary to address the complex array of privacy, security, trust, and power issues at play. Our above discussion underscores the responsibility of HCI and design researchers to identify potential limits to our own expertise and interventions. This may also entail imagining ways to encourage users to limit or relinquish use of surveillant devices [12], and adopting an "undesign" [100, 129] perspective that pushes back against the assumption that SHCs are a necessary or inevitable facet of daily life. We conducted our study in the United States, where regulations on recording vary by state; international laws vary even further. With such considerations and limitations in mind, we provide three specific regulatory implications from our work:

Policy must consider privacy and data collection in contextual ways. Our findings depict a diversity of uses of smart home cameras. This evolving multi-functionality suggests that general regulations for devices (policies affecting all smart cameras) might be overly broad and can neglect to consider the contextual norms that correspond to different types of social interactions and practices (e.g., physical security surveillance is different from care-based surveillance, and so forth). As such, Nissenbaum's contextual integrity approach is pertinent to consider how, and which data flows are appropriate for these varied use cases [94].

More regulations are necessary to stop deceptive design practices in smart cameras. In findings about frontend and backend users, participants derived inferences about backend processes with their SHC data based on company subscription plans, creating a "What you see on your interface is all there is" model, when in actuality the correct mental model is "What you see is just your interface" (the company can see so much more). This asymmetry has the potential to mislead users, conveying incorrect mental models about backend elements (such as what data is being collected or stored). At times, this practice may constitute what legal scholar Woodrow Hartzog refers to as "deceptive design" [64]. However, the mismatch between what a user sees on their interface and what a company is doing behind the scenes is not necessarily deceptive or a "dark design pattern" [61], and it is common for designers to deliberately shield users from unnecessary or confusing information. However, in instances where such practices are deemed deceptive, one might turn to US consumer protection laws, in which the Federal Trade Commission may formally label these design choices as "deceptive" to create regulatory enforcement against companies employing these practices.

Law and policy need to recognize new mechanisms for legally collecting or using data beyond current individually focused privacy notice and consent models. Through illuminating the various interhousehold dynamics associated with monitoring and surveillance uses of smart home cameras, we assert that privacy legislation needs to consider group and non-primary user issues differently. As SHCs enable non-primary users' data to be collected and shared by others, we must reconsider the prevailing *individual* consent models for privacy. This is aligned with Levy and Baroca's concept of privacy dependencies, which illustrates how other's actions may violate one's privacy (and vice versa) [9]. They impart, "privacy dependencies should thus not only call into question notice and choice as a model for privacy regulation; they should force us to abandon the naïve hope that solidarity can help rescue informed consent by clarifying the degree to which our privacy choices implicate others" (p. 615). Therefore, as our work details the myriad interdependencies, relational uses, and power asymmetries of SHCs, we understate the need to establish privacy paradigms beyond individual approaches for notice and consent—indicating the consequential and dynamic implications for monitoring and surveillance as perpetuated by smart home cameras.

10 CONCLUSION

Our work provides an empirical investigation into the various surveillance use cases of the consumer smart home camera (SHC), an increasingly popular new category of smart home products. Through interviews with 14 SHC users, we unravel privacy tensions and power imbalances related to the household dynamics of living with these perceptually powerful and spatially sensitive devices. We observed how users employed the range of sensing capabilities in smart cameras to extend their perception, and to engage in various forms of monitoring and surveillance that includes but goes beyond conventional security uses cases such as deterring or catching intruders.

Our findings impart several concepts for classifying these uses of SHCs, as we categorize the different types of everyday monitoring and surveillance activities participants engaged in. We also discuss asymmetrical and power-laden implications of these uses and the tensions created between primary and non-primary users. From these insights, we conclude with design considerations for balancing primary and non-primary users' privacy, and implications for law and policy regulations with smart camera technology. Overall, we hope that our investigation paves new directions for HCI, privacy, and IoT, as we stress the need to continue to examine and critique new forms of surveillance afforded by emerging ubiquitous technologies such as the smart home camera.

ACKNOWLEDGMENTS

We express our sincere gratitude to our study participants for generously sharing their time and perspectives, and to our anonymous reviewers for providing helpful comments and suggestions. This study was funded by a Mozilla Research Grant 2018H2, the National Science Foundation under awards IIS-1947696, IIS-155367, and IIS-2142795, and the National Science Foundation Graduate Research Fellowship under Grant No. DGE-1762114.

REFERENCES

[1] William Ablondi. 2018. Smart Home Reports. Strategy Analytics. Retrieved from https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/reports/report-detail/global-smart-home-surveillance-camera-market-forecast-2012-to-2023?slid=918459&spg=4

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and others. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. ACM Comput. Surv. CSUR 50, 3 (2017), 1–41.

[3] Shane Ahern, Dean Eckles, Nathaniel S Good, Simon King, Mor Naaman, and Rahul Nair. 2007. Over-exposed? Privacy patterns and considerations in online and mobile photo sharing. In Proceedings of the SIGCHI conference on Human factors in computing systems, 357–366.

[4] 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 (2020), 1–28.

[5] Ryan Aipperspach, Ben Hooker, and Allison Woodruff. 2008. The heterogeneous home. In Proceedings of the 10th international conference on Ubiquitous computing, 222–231.

[6] Tawfiq Ammari, Jofish Kaye, Janice Y. Tsai, and Frank Bentley. 2019. Music, Search, and IoT: How People (Really) Use Voice Assistants. ACM Trans. Comput.-Hum. Interact. 26, 3 (June 2019), 1–28.

[7] Louise Amoore. 2020. Cloud ethics. Duke University Press.

[8] Mike Ananny and Kate Crawford. 2018. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media Soc. 20, 3 (2018), 973–989.

[9] Solon Barocas and Karen Levy. 2020. Privacy Dependencies. Wash. Law Rev. 95, 2 (June 2020), 555.

[10] Eric PS Baumer. 2015. Reflective informatics: conceptual dimensions for designing technologies of reflection. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 585–594.

[11] Eric P.S. Baumer. 2015. Usees. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM, Seoul Republic of Korea, 3295–3298.

[12] Eric PS Baumer, Phil Adams, Vera D Khovanskaya, Tony C Liao, Madeline E Smith, Victoria Schwanda Sosik, and Kaiton Williams. 2013. Limiting, leaving, and (re) lapsing: an exploration of facebook non-use practices and experiences. In Proceedings of the SIGCHI conference on human factors in computing systems, 3257–3266.

[13] Rosanna Bellini, Angelika Strohmayer, Patrick Olivier, and Clara Crivellaro. 2019. Mapping the Margins: Navigating the Ecologies of Domestic Violence Service Provision. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, Glasgow Scotland Uk, 1–13.

[14] Erin Beneteau, Yini Guan, Olivia K. Richards, Mingrui Ray Zhang, Julie A. Kientz, Jason Yip, and Alexis Hiniker. 2020. Assumptions Checked: How Families Learn About and Use the Echo Dot. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4, 1 (March 2020), 1–23.

[15] Jesse Josua Benjamin, Arne Berger, Nick Merrill, and James Pierce. 2021. Machine Learning Uncertainty as a Design Material: A Post-Phenomenological Inquiry. Proc. 2021 CHI Conf. Hum. Factors Comput. Syst. (May 2021), 1–14.

[16] Frank Bentley, Chris Luvogt, Max Silverman, Rushani Wirasinghe, Brooke White, and Danielle Lottridge. 2018. Understanding the Long-Term Use of Smart Speaker Assistants. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 3 (September 2018), 1–24.

[17] Francine Berman and Vinton G. Cerf. 2017. Social and ethical behavior in the internet of things. Commun. ACM 60, 2 (January 2017), 6–7.

[18] Clara Berridge, Jodi Halpern, and Karen Levy. 2019. Cameras on beds: The ethics of surveillance in nursing home rooms. AJOB Empir. Bioeth. 10, 1 (January 2019), 55–62.

[19] Susanne Bødker. 2006. When second wave HCI meets third wave challenges. In Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles, 1–8.

[20] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. The New York Times. Retrieved from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

[21] Phoebe Braithwaite. 2018. Smart home tech is being turned into a tool for domestic abuse. Wired UK. Retrieved from https://www.wired.co.uk/article/internet-of-things-smart-home-domestic-abuse

[22] Simone Browne. 2015. Dark Matters: On the Surveillance of Blackness. Duke University Press.

[23] Jed R. Brubaker, Gina Venolia, and John C. Tang. 2012. Focusing on shared experiences: moving beyond the camera in video communication. In Proceedings of the Designing Interactive Systems Conference on - DIS '12, ACM Press, Newcastle Upon Tyne, United Kingdom, 96.

[24] AJ Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. 2013. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In Proceedings of the 2013 conference on Computer supported cooperative work, 693–700.

[25] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home automation in the wild: challenges and opportunities. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Vancouver BC Canada, 2115–2124.

[26] Taina Bucher. 2012. Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media Soc. 14, 7 (2012), 1164–1180.

[27] Will Burns. 2018. The "Nestie Awards" From Nest Is A Content Idea Firing On All Cylinders. Forbes. Retrieved from https://www.forbes.com/sites/willburns/2018/03/02/the-nestie-awards-from-nest-is-a-content-idea-firing-on-all-cylinders/

[28] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation inaction or in action? the role of user experience in the security and privacy design of smart home cameras. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), 185–204.

[29] 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, ACM, Yokohama Japan, 1–16.

[30] 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, 1–12.

[31] 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, ACM, San Diego CA USA, 823–836.

[32] Marshini Chetty, Ja-Young Sung, and Rebecca E. Grinter. 2007. How Smart Homes Learn: The Evolution of the Networked Home and Household. In UbiComp 2007: Ubiquitous Computing, John Krumm, Gregory D. Abowd, Aruna Seneviratne and Thomas Strang (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 127–144.

[33] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a glass house: a survey of private moments in the home. In Proceedings of the 13th international conference on Ubiquitous computing - UbiComp '11, ACM Press, Beijing, China, 41.

[34] Danielle Keats Citron. 2014. Hate crimes in cyberspace. Harvard University Press.

[35] Andy Crabtree, Peter Tolmie, and Will Knight. 2017. Repacking 'Privacy' for a Networked World. Comput. Support. Coop. Work CSCW 26, 4 (December 2017), 453–488.

[36] Kate Crawford. 2021. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press.

[37] Christopher Dandeker. 2006. Surveillance and Military Transformation: Organizational Trends in Twenty First Century Armed Services. New Polit. Surveill. Visibility (2006), 225–249.

[38] Dries De Roeck, Karin Slegers, Johan Criel, Marc Godon, Laurence Claeys, Katriina Kilpi, and An Jacobs. 2012. I would DiYSE for it! A manifesto for do-it-yourself internet-of-things creation. In NordiCHI '12 Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design, AMC, 170–179.

[39] Gilles Deleuze. 1992. Postscript on the Societies of Control. October 59, (1992), 3–7.

[40] George Demiris, Brian K Hensel, Marjorie Skubic, and Marilyn Rantz. 2008. Senior residents' perceived need of and preferences for "smart home" sensor technologies. Int. J. Technol. Assess. Health Care 24, 1 (2008), 120–124.

[41] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: perspectives on recording and privacy-mediating technologies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Toronto Ontario Canada, 2377–2386.

[42] Audrey Desjardins, Jeremy E. Viny, Cayla Key, and Nouela Johnston. 2019. Alternative Avenues for IoT: Designing with Non-Stereotypical Homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19, ACM Press, Glasgow, Scotland Uk, 1–13.

[43] Paul Dourish and Genevieve Bell. 2011. Divining a digital future: Mess and mythology in ubiquitous computing. Mit Press.

[44] Serge Egelman and Eyal Peer. 2015. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In Proceedings of the 2015 New Security Paradigms Workshop, ACM, Twente Netherlands, 16–28.

[45] Daniel Fallman. 2011. The new good: exploring the potential of philosophy of technology to contribute to human-computer interaction. In Proceedings of the SIGCHI conference on human factors in computing systems, 1051–1060.

[46] Michel Foucault. 2012. Discipline and punish: The birth of the prison. Vintage.

[47] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal QC Canada, 1–13.

[48] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), 21–40.

[49] Ester Fritsch, Irina Shklovski, and Rachel Douglas-Jones. 2018. Calling for a Revolution: An Analysis of IoT Manifestos. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal QC Canada, 1–13.

[50] Christian Fuchs. 2010. How Can Surveillance Be Defined? Remarks on Theoretical Foundations of Surveillance Studies. The Internet (2010), 24.

[51] Kit Galloway and Sherrie Rabinowitz. A Hole-In-Space, 1980. Retrieved from http://www.ecafe.com/getty/HIS/index.html

[52] William W Gaver. 2006. The video window: my life with a ludic system. Pers. Ubiquitous Comput. 10, 2–3 (2006), 60–65.

[53] William W. Gaver, John Bowers, Kirsten Boehner, Andy Boucher, David W.T. Cameron, Mark Hauenstein, Nadine Jarvis, and Sarah Pennington. 2013. Indoor weather stations: investigating a ludic approach to environmental HCI through batch prototyping. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Paris France, 3451–3460.

[54] Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, and Kate Crawford. 2018. Datasheets for datasets. ArXiv Prepr. ArXiv180309010 (2018).

[55] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, Glasgow Scotland Uk, 1–13.

[56] Chris Gilliard and David Golumbia. 2021. Luxury Surveillance. Real Life. Retrieved from https://reallifemag.com/luxury-surveillance/

[57] Barney G Glaser and Anselm L Strauss. 2017. Discovery of grounded theory: Strategies for qualitative research. Routledge.

[58] Jake Goldenfein, Deirdre K Mulligan, Helen Nissenbaum, and Wendy Ju. 2020. Through the Handoff Lens: Competing Visions of Autonomous Futures. Berkeley Tech LJ 35, (2020), 835.

[59] Ellen P Goodman and Julia Powles. 2019. Urbanism under Google: Lessons from Sidewalk Toronto. Fordham Rev 88, (2019), 457.

[60] Stephen Graham and David Wood. 2003. Digitizing Surveillance: Categorization, Space, Inequality. Crit. Soc. Policy 23, 2 (May 2003), 227–248.

[61] Colin M Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–18.

[62] Byung-Chul Han. 2017. In the swarm: Digital prospects. MIT Press.

[63] Jenny Hansson. Fearless feline chases coyote in Portland neighborhood. KOIN.com. Retrieved from https://www.koin.com/news/animals/fearless-feline-chases-coyote-in-portland-neighborhood/

[64] Woodrow Hartzog. 2018. Privacy's blueprint. Harvard University Press.

[65] Adam Harvey. 2020. CV Dazzle: Computer Vision Dazzle Camouflage. Retrieved from https://cvdazzle.com/

[66] Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar. 2008. Challenges in universally usable privacy and security. In Symposium On Usable Privacy and Security (SOUPS).

[67] Sun-ha Hong. 2020. Technologies of Speculation. New York University Press.

[68] Heather A Horst, Cherry Baylosis, and Sheba Mohammid. 2021. Looking professional: How women decide what to wear with and through automated technologies. Convergence 27, 5 (October 2021), 1250–1263.

[69] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Cr, and All Apu Kapadia. Privacy Behaviors of Lifeloggers using Wearable Cameras. UbiComp, 571–582.

[70] Tung-Hui Hu. 2015. A Prehistory of the Cloud. MIT press.

[71] Don Ihde. 1990. Technology and the lifeworld: From garden to earth. (1990).

[72] Alan Jacobs. Attending to Technology: Theses for Disputation. The New Atlantis. Retrieved from https://www.thenewatlantis.com/publications/attending-to-technology-theses-for-disputation

[73] Steven Johnson, Irene Rae, Bilge Mutlu, and Leila Takayama. 2015. Can You See Me Now?: How Field of View Affects Collaboration in Robotic Telepresence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM, Seoul Republic of Korea, 2397–2406.

[74] Daniel Kahneman. 2011. Thinking, Fast and Slow. Macmillan.

[75] Evangelos Karapanos, Rúben Gouveia, Marc Hassenzahl, and Jodi Forlizzi. 2016. Wellbeing in the making: peoples' experiences with wearable activity trackers. Psychol. Well-Being 6, 1 (2016), 1–17.

[76] Lauren Kilgour. 2020. The ethics of aesthetics: Stigma, information, and the politics of electronic ankle monitor design. Inf. Soc. 36, 3 (May 2020), 131–146.

[77] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan, 1–14.

[78] Sandjar Kozubaev, Fernando Rochaix, Carl DiSalvo, and Christopher A. Le Dantec. 2019. Spaces and Traces: Implications of Smart Technology in Public Housing. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, Glasgow Scotland Uk, 1–13.

[79] Joshua A Kroll, Joanna Huey, Solon Barocas, Edward W Felten, Joel R Reidenberg, David G Robinson, and Harlan Yu. Accountable Algorithms. Univ. Pa. Law Rev. 165, 74.

[80] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018), 1–31.

[81] Roxanne Leitão. 2018. Digital Technologies and their Role in Intimate Partner Violence. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal QC Canada, 1–6.

[82] Melissa Lemieux. 2019. Watch the Viral Video of a Small Boy Filling an Empty Trick-or-Treat Bowl With His Halloween Candy. Newsweek. Retrieved from https://www.newsweek.com/watch-viral-video-small-boy-filling-empty-trick-treat-bowl-his-halloween-candy-1469331

[83] Karen E C Levy. 2014. Intimate Surveillance. Ida. Law Rev. 51, (2014), 679.

[84] Yanni Alexander Loukissas. 2019. All data are local: Thinking critically in a data-driven society. MIT Press.

[85] Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users protect their privacy if they can: Determinants of webcam covering behavior. In Proceedings of the European Workshop on Usable Security at the Privacy Enhaning Technologies Symposium (EuroSEC'16)(EuroUSEC'16). Internet Society, Reston, VA.

[86] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. Proc. Priv. Enhancing Technol. 2019, 4 (October 2019), 250–271.

[87] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. Proc. Priv. Enhancing Technol. 2020, 2 (April 2020), 436–458.

[88] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, ACM, Denver Colorado USA, 2189–2201.

[89] 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, ACM, Denver Colorado USA, 5197–5207.

[90] Sarah Mennicken and Elaine M Huang. 2012. Hacking the natural habitat: an in-the-wild study of smart homes, their development, and the people who live in them. In International conference on pervasive computing, Springer, 143–160.

[91] Jochen Meyer, Jochen Schnauber, Wilko Heuten, Harm Wienbergen, Rainer Hambrecht, Hans-Jürgen Appelrath, and Susanne Boll. 2016. Exploring Longitudinal Use of Activity Trackers. In 2016 IEEE International Conference on Healthcare Informatics (ICHI), IEEE, 198–206.

[92] Matthew B Miles and A Michael Huberman. 1994. Qualitative data analysis: An expanded sourcebook. sage.

[93] Elizabeth C Nelson, Tibert Verhagen, and Matthijs L Noordzij. 2016. Health empowerment through activity trackers: An empirical smart wristband study. Comput. Hum. Behav. 62, (2016), 364–374.

[94] Helen Nissenbaum. 2004. Privacy as contextual integrity. Wash Rev 79, (2004), 119.

[95] William Odom. 2015. Understanding Long-Term Interactions with a Slow Technology: an Investigation of Experiences with FutureMe. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM, Seoul Republic of Korea, 575–584.

[96] 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, 41–50.

[97] Kentrell Owens, Camille Cobb, and Lorrie Cranor. 2021. "You Gotta Watch What You Say": Surveillance of Communication with Incarcerated People. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan, 1–18.

[98] Seung-min Park, Daeyoun D Won, Brian J Lee, Diego Escobedo, Andre Esteva, Amin Aalipour, T Jessie Ge, Jung Ha Kim, Susie Suh, Elliot H Choi, and others. 2020. A mountable toilet system for personalized health monitoring via the analysis of excreta. Nat. Biomed. Eng. 4, 6 (2020), 624–635.

[99] S Tejaswi Peesapati, Victoria Schwanda, Johnathon Schultz, Matt Lepage, Soyae Jeong, and Dan Cosley. 2010. Pensieve: supporting everyday reminiscence. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2027–2036.

[100] James Pierce. 2012. Undesigning technology: considering the negation of design by design. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 957–966.

[101] 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 (CHI '19), Association for Computing Machinery, New York, NY, USA, 1–14.

[102] 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, ACM, Honolulu HI USA, 1–19.

[103] Irene Rae, Gina Venolia, John C. Tang, and David Molnar. 2015. A Framework for Understanding and Designing Telepresence. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM, Vancouver BC Canada, 1552–1566.

[104] Horst WJ Rittel and Melvin M Webber. 1974. Wicked Problems. Man-Made Futur. 26, 1 (1974), 272–280.

[105] Gilad Rosner and Erin Kenneally. 2018. Clearly opaque: Privacy risks of the internet of things. In Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum.

[106] James B Rule. 2007. Privacy in peril: How we are sacrificing a fundamental right in exchange for security and convenience. Oxford University Press.

[107] Pedro Sanches, Vasiliki Tsaknaki, Asreen Rostami, and Barry Brown. 2020. Under Surveillance: Technology Practices of those Monitored by the State. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, Honolulu HI USA, 1–13.

[108] Christine Satchell and Paul Dourish. 2009. Beyond the user: use and non-use in HCI. In Proceedings of the 21st annual conference of the Australian computer-human interaction special interest group: Design: Open 24/7, 9–16.

[109] Johann Schrammel, Christina Köffel, and Manfred Tscheligi. 2009. Personality traits, usage patterns and information disclosure in online communities. In In BCS HCI '09: Proceedings of the 2009 British Computer Society Conference on Human-Computer Interaction, 169–174.

[110] Phoebe Sengers, Kirsten Boehner, Shay David, and Joseph'Jofish' Kaye. 2005. Reflective Design. In Proceedings of the 4th decennial conference on Critical computing: between sense and sensibility, 49–58.

[111] William Seymour, Reuben Binns, Petr Slovak, Max Van Kleek, and Nigel Shadbolt. 2020. Strangers in the Room: Unpacking Perceptions of "Smartness" and Related Ethical Concerns in the Home. In Proceedings of the 2020 ACM Designing Interactive Systems Conference, ACM, Eindhoven Netherlands, 841–854.

[112] Mark Shepard. Sentient City Survival Kit. Retrieved March 9, 2022 from http://survival.sentientcity.net/umbrella.html

[113] Samarth Singhal, Carman Neustaedter, Thecla Schiphorst, Anthony Tang, Abhisekh Patra, and Rui Pan. 2016. You are Being Watched: Bystanders' Perspective on the Use of Camera Devices in Public Spaces. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, ACM, San Jose California USA, 3197–3203.

[114] Robert H Sloan and Richard Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. J High Tech L 14, (2014), 370.

[115] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. Harv Rev 126, (2012), 1880.

[116] Anne Spaa, Abigail Durrant, Chris Elsden, and John Vines. 2019. Understanding the Boundaries between Policymaking and HCI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–15.

[117] Luke Stark and Karen Levy. 2018. The surveillant consumer. Media Cult. Soc. 40, 8 (November 2018), 1202–1220.

[118] Yolande Strengers, Jenny Kennedy, Paula Arcari, Larissa Nicholls, and Melissa Gregg. 2019. Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, Glasgow Scotland Uk, 1–13.

[119] Tactical Tech. The Glass Room – Looking into your online life. Retrieved from https://www.theglassroom.org/en/home/

[120] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing Relations between Humans and Sensing Devices through an Anthropomorphic Webcam. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, Yokohama Japan, 1–13.

[121] Emily Troshynski, Charlotte Lee, and Paul Dourish. 2011. Accountabilities of presence: reframing location-based systems. Droit Cult. Rev. Int. Interdiscip. 61 (2011), 171–193.

[122] Khai Truong, Shwetak Patel, Jay Summet, and Gregory Abowd. 2005. Preventing Camera Recording by Designing a Capture-Resistant Environment.

[123] 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, ACM, Seattle Washington, 129–139.

[124] Peter-Paul Verbeek. 2005. What Things Do: Philosophical Reflections on Technology, Agency, and Design. Penn State University Press.

[125] Ron Wakkary. 2021. Things We Could Design: For More Than Human-Centered Worlds. MIT Press, Cambridge, MA, USA.

[126] Ron Wakkary and Leah Maestri. 2007. The resourcefulness of everyday design. In Proceedings of the 6th ACM SIGCHI conference on Creativity & Cognition (C&C '07), Association for Computing Machinery, New York, NY, USA, 163–172.

[127] Jayne Wallace, Jon Rogers, Michael Shorter, Pete Thomas, Martin Skelly, and Richard Cook. 2018. The SelfReflector: Design, IoT and the High Street. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, Montreal QC Canada, 1–12.

[128] Yang Wang. 2017. The Third Wave?: Inclusive Privacy and Security. In Proceedings of the 2017 New Security Paradigms Workshop, ACM, Santa Cruz CA USA, 122–130.

[129] Kelly Widdicks, Tina Ringenson, Daniel Pargman, Vishnupriya Kuppusamy, and Patricia Lago. 2018. Undesigning the Internet: An Exploratory Study of Reducing Everyday Internet Connectivity. In EPiC Series in Computing, EasyChair, 384–397.

[130] Oscar Williams. 2017. Nestie Awards 2017: Hilarious Moments Caught On Home Security Cameras. HuffPost UK. Retrieved from https://www.huffingtonpost.co.uk/entry/nestie-awards-2017-hilarious-moments-caught-on-home-security-cameras_uk_58c6a2d6e4b0d1078ca806f4

[131] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19), Association for Computing Machinery, New York, NY, USA, 1–17.

[132] Allison Woodruff, Sally Augustin, and Brooke Foucault. 2007. Sabbath Day Home Automation: "It's Like Mixing Technology and Religion". In In Proceedings of the 2007 Conference on Human Factors in Computing Systems (CHI 2007), ACM Press.

[133] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum.-Comput. Interact. 3, CSCW (November 2019), 1–24.

[134] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, ACM, Denver Colorado USA, 6777–6788.

[135] MinYoung Yoo, William Odom, and Arne Berger. 2021. Understanding Everyday Experiences of Reminiscence for People with Blindness: Practices, Tensions and Probing New Design Possibilities. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21), Association for Computing Machinery, New York, NY, USA, 1–15.

[136] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security & Privacy Concerns with Smart Homes. 17.

[137] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. Proc. ACM Hum.-Comput. Interact. 2, CSCW (November 2018), 200:1-200:20.

[138] Shoshana Zuboff. 2018. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (1st ed.).

[139] 2016. 61% Of Smart-Home Revenue Came From Security Cameras In The Last Year. TWICE. Retrieved from https://www.twice.com/news/61-smart-home-revenue-came-security-cameras-last-year-62631