Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras

James Pierce[1,2,4], Claire Weizenegger[1], Parag Nandi[2,4], Isha Agarwal[1,4], Gwenna Gram[1], Jade Hurle[1], Betty Lo[1], Aaron Park[1], Aivy Phan[1], Mark Shumskiy[1], Grace Sturlaugson[1]

[1] Division of Design, School of Art + Art History + Design, [2] Human Centered Design and Engineering, [3] MHCI+D Program, [4] DUB Group

Abstract

Many consumer Internet Things (IoT) devices involve spatial sensors such as cameras and microphones. These affect the privacy of nearby people. A prime example is smart home security cameras. We present our work developing scenarios, use cases, and design proposals for addressing smart camera privacy. Preliminary findings from a concept evaluation with 11 participants is presented. The outcomes of this research through design project foreground the importance and challenges of designing to support the privacy of nearby users. We outline actionable design responses while also raising limitations of technology approaches alone to address these issues.

Authors Keywords: Interaction Design; Smart home; Internet of Things (IoT); Privacy; Research through Design

DIS '22, June 13–17, 2022, Virtual Event, Australia

ACM ISBN 978-1-4503-9358-4/22/06.
https://doi.org/10.1145/3532106.3535195

Introduction

Smart devices with cameras, microphones, location tracking, and other spatial sensing capabilities invariably impact the privacy of people nearby. A prime example is smart home security cameras. These devices are used both deliberately and incidentally to monitor guests, neighbors, domestic workers, family members, roommates, and passersby [3,7,12,14,24,29,33,36,37,38]. These nearby users lack the high degrees of control, feedback, awareness, consent, and benefits of use enjoyed by primary users. However the vast majority of privacy features and safeguards are designed not for those nearby, but rather for the primary users who own and operate the devices. Relatively few design interventions exist, either in consumer applications or research prototypes, that specifically address the privacy of adjacent actors of smart sensing devices.

Researchers are increasingly calling for stronger consideration of various stakeholders beyond the primary user [2,3,10,15,19,24,28,29,33,36]. Yet while many pages have been written outlining empirical insights and general design recommendations, there is a conspicuous lack of detailed design work that addresses these issues. As it turns out, designing interactive systems that directly improve adjacent actor privacy is very difficult, not least because it requires navigating competing interests among primary users and other stakeholders. Furthermore, adjacent users often lack access to critical interface elements such as feedback and privacy settings.

Prior work has referred to these stakeholders as bystanders [3,36] or incidental users [17]. We consider bystander and incidental users as important subsets of a larger space we refer to as *adjacent actors*. For simplicity, we sometimes alternatively refer to adjacent actors as *nearby users*, even though the term user may be misleading if it refers to a subject with little control or awareness.

In our framework, bystanders and incidental users both lie somewhere between a *co-user* with some control and benefits, and a *surveilled subject*, who may have little control and suffer significant harms. If a camera owner accidentally records a person walking down the street, we consider that person a *bystander* in that they are present but not actively involved in the use of the device. However a nanny, child, or Airbnb guest who is deliberately surveilled by the camera owner is no longer merely a bystander but rather a surveilled subject (or, a *usee* [1]). Similarly, if a camera owner opportunistically spies on their neighbor [33], that person is less a bystander than a non-consenting subject. A delivery driver who stands in front of a doorbell knowing the owner may see them is also not simply a bystander but an *indirect or incidental user*. Complicating matters further, these roles are fluid and contingent. For example, the primary owner of a camera can later become a surveilled subject if their spouse with co-user access uses the system to spy on them.

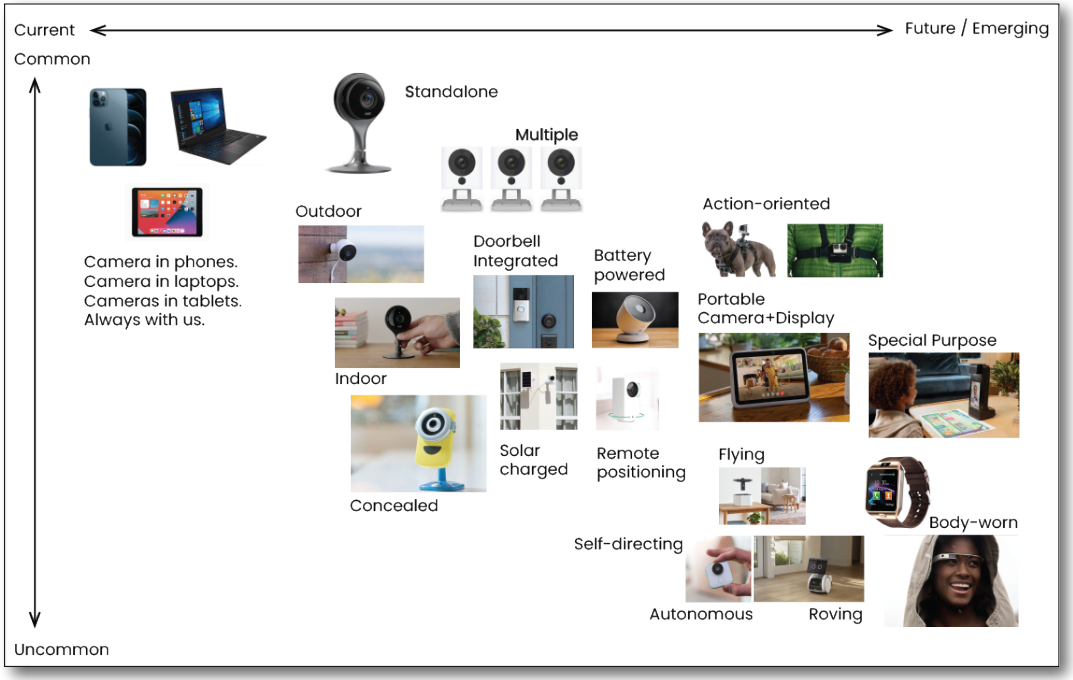
We present an interdisciplinary research through design inquiry into adjacent actor privacy for smart home cameras. Drawing on our team's expertise in interactive and industrial design, and usable privacy and security, we report our ongoing work mapping the design space and crafting interventions. We present detailed design proposals and show our work [11,18] by revealing design frameworks and insights that led us to our designs, and demonstrating a process others may replicate or adapt. We conclude with preliminary findings from a concept evaluation with 11 participants, including adjacent actors such as a pet sitter, house-sitter, roommate, and Airbnb guest. Our *supplemental documentation* offers a fuller picture into work.

Mapping the Landscape: Smart Cams and Privacy Implications
We focused on smart cameras (which often have integrated microphones) because they represent a major source of privacy issues for both primary users and adjacent actors [7,29,33]. We first sought to understand different types of smart cameras and their affects on adjacent actor privacy. One framework we developed to make sense of this vast landscape of smart camera products was a smart cam evolution map. We loosely plotted camera devices along two axes: common versus uncommon, and current versus emerging. This map was useful in numerous ways, including enabling us to tease apart two other frameworks described below.

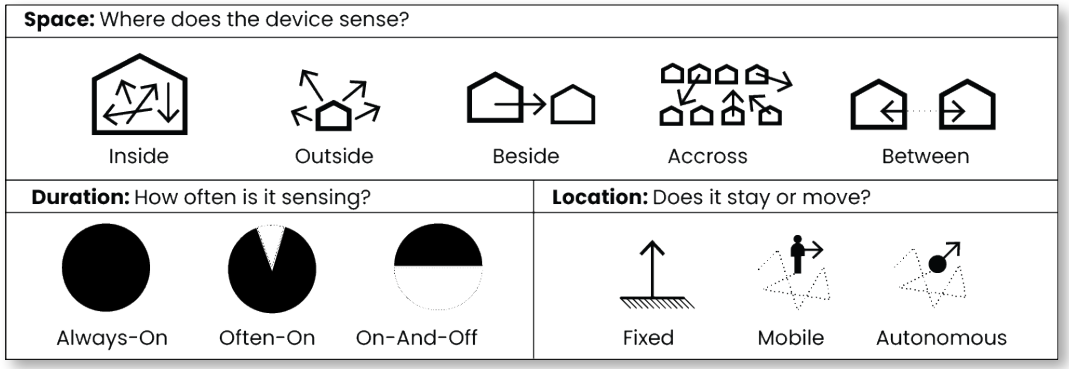
3 Spatial and Temporal Dimensions of Smart Cameras
We identified 3 dimensions with significant implications for adjacent actor privacy. *(1) Where does the device sense?* For example, a security camera inside a home is very different from a camera outside the home. And both differ from a camera for communicating between homes, such as a webcam. *(2) How often is the device sensing?* Security cameras may be on for long durations ("always-on" or "often-on"), whereas camera phones and webcams cameras are only on for specific tasks ("on-and-off"). *(3) Does the camera stay or move?* Many security cameras remain relatively fixed ("stationary"). Battery powered cameras are moved around ("mobile"). Drone and robot cameras move with self-direction ("autonomous").

4 Smart Camera Groups
From our evolutionary camera map, we distinguished 4 key groups of smart cameras. We ultimately focused on designing for standalone cameras (Group 1) because these devices are both very common and significantly impact adjacent actor privacy. However we kept an eye out for overlapping opportunities to improve privacy for other camera groups.

Group 1: Stationary Standalone Smart Cameras. These cameras are stationary or semi-stationary, and typically used in an always-on or often-on state. Consequently, they are very likely to affect nearby actor privacy. *Group 2: Integrated Cameras on Portable Devices.* These cameras are often mobile, which can increase privacy concerns for adjacent actors. But overall they tend to be less privacy-invasive because they are task-oriented, and cameras and mics are disabled when not in use. These devices are also not specifically designed for surveillance. *Group 3: Autonomously Mobile Smart Cameras.* These devices can create significant adjacent actor privacy concerns all types of adjacent actors. However these devices are new, expensive, and it is unclear whether they will become as common as standalone smart home cameras. *Group 4: Wearable Smart Cameras.* These include smart glasses and action cameras. Action cameras are typically used in an on-and-off manner for specialized activities, often outdoor adventures. Smart glasses may involve often-on cameras used across many everyday contexts.



Evolution of smart cameras: From common and current, to uncommon and emerging.



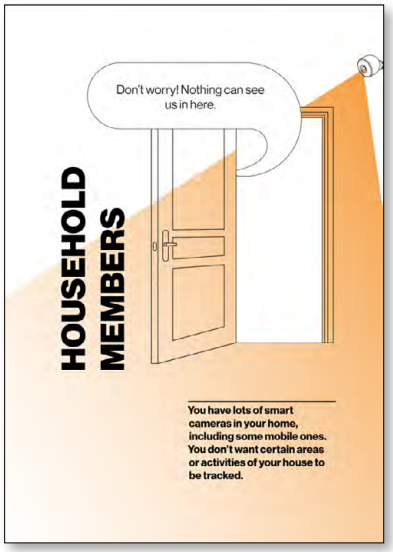
3 Camera dimensions: Space where it senses, duration of sensing, and location of sensing.

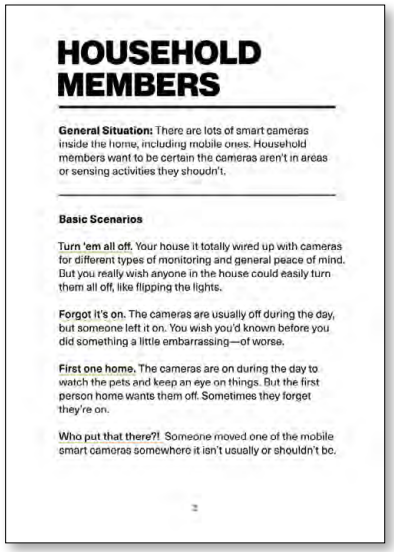
4 Camera Groups: Standalone, Integrated into Portable Devices, Autonomous, and Wearable

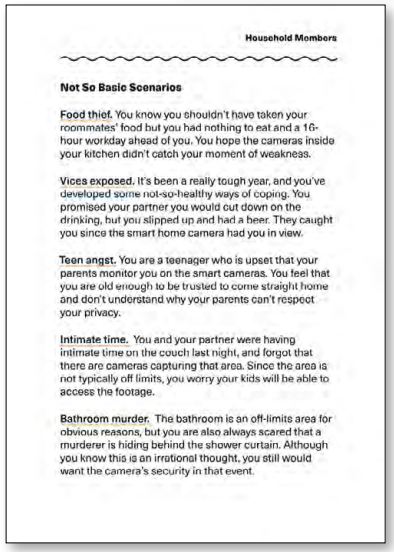
Setting the Stage: Identifying Situations, Scenarios, and Scenes

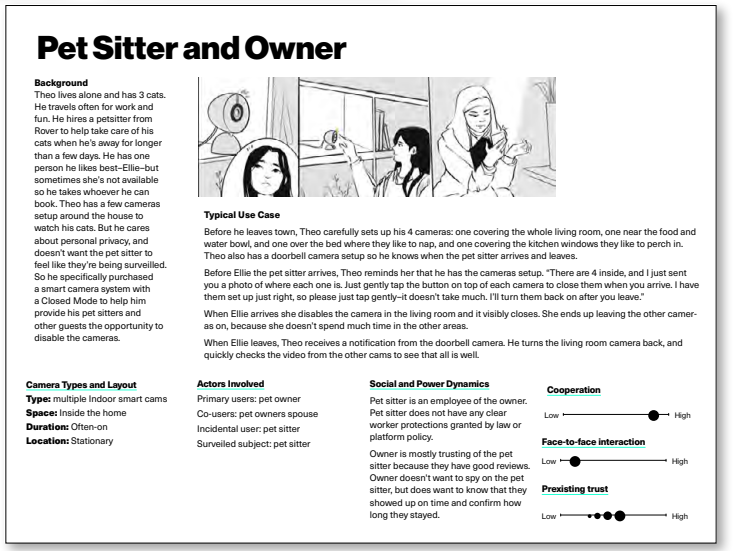
Before we began developing design concepts in earnest, we iteratively developed many use cases and scenarios [e.g., 6,21]. These scenarios allowed us to imagine a diversity of contexts in which better privacy features might be desired. For example, we imagined cooperate situations where the first person to arrive home wanted to ensure all the cameras were turned off. We also imagined non-cooperative scenarios, such as a neighbor who refused to turn their camera away from your home. Below we outline several categories of scenarios that we used to curate and organize our work.

To generate scenarios, we relied on a mixture of firsthand experience, secondary literature, and interviews with smart home camera users for a separate research project [33]. Some scenarios were directly based on real experiences, while others were fictionalized hypotheticals. We curated a range of scenarios and compiled them into a booklet. We used these scenarios to inform and inspire our design interventions. The booklet also served as a valuable tool for facilitating collaboration and onboarding new team members.









Our use cases emergently settled into a hierarchy of 3 levels of specificity: general situations, specific scenarios, and detailed scenes.

General situations describe a broad category of activities where adjacent users may be negatively affected by smart cameras. **Example:** "Household Members - There are lots of smart cameras inside the home. Household members want to be certain the cams aren't in areas or sensing activities they shouldn't."

Basic specific scenarios describe general use cases or contexts where adjacent user privacy is at stake. **Example:** "Forgot it's on. The cameras are usually off during the day, but someone left it on. You wish you'd known before you did something a little embarrassing—or worse."

Not so basic specific scenarios describe atypical, idiosyncratic, even slightly absurd use cases. **Example:** "Vices. It's been a tough year, and you've developed some not-so-healthy ways of coping. You promised your partner you'd drink less, but you slipped They caught you on camera. Whoops."

Detailed scenes are longer text-based narratives or visual storyboards that expand upon specific scenarios with detail and nuance. For selected scenes, we translated our written stories into 1-page documents containing information such as level of cooperation and pre-existing trust between users. We found these documents useful as an alternative to conventional user personas. Instead of focusing on a single user, these detailed scenes encapsulate interactions *between* primary users and adjacent actors.

Developing Design Proposals

The scenarios and frameworks described on the previous pages helped us understand needs and opportunities to improve privacy and trust for adjacent actors. Our next step was to actually design detailed and potentially feasible design responses—a major gap we identified across both consumer product development and academic research.

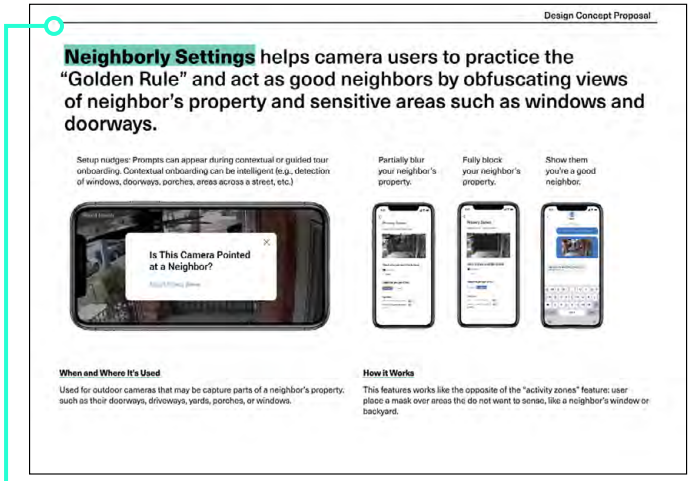
We initially developed approximately 50 design ideas addressing a range of camera types (Groups 1–4 cameras) and adjacent actor scenarios. We then narrowed most of our concepts to Stationary Standalone Cameras (Group 1) because these cameras are very common and carry significant privacy implications for adjacent actors. Ultimately we developed two sets of design proposals, which we elaborate in the remainder of this paper.

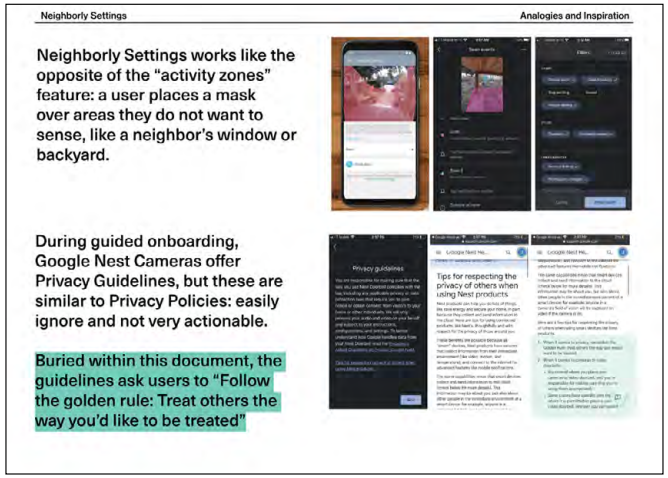
Design Proposals (For Us)

For our top candidates, we developed more detailed design proposals documents. These design proposals were internal documents we used to capture and communicate our design work within the research team. Each proposal includes a summary of "When and Where It's Used", "How it Works," and the key features and functions. A supplemental section of each proposal documents examples that inspired and informed the design or provide helpful analogies.

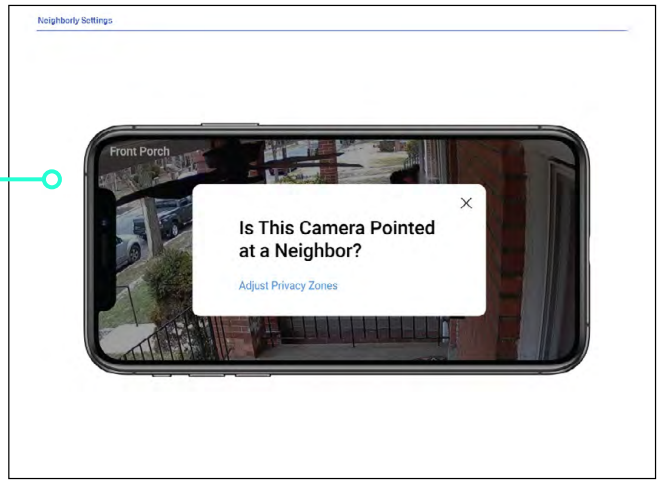
Simplified Proposals (For Participants)

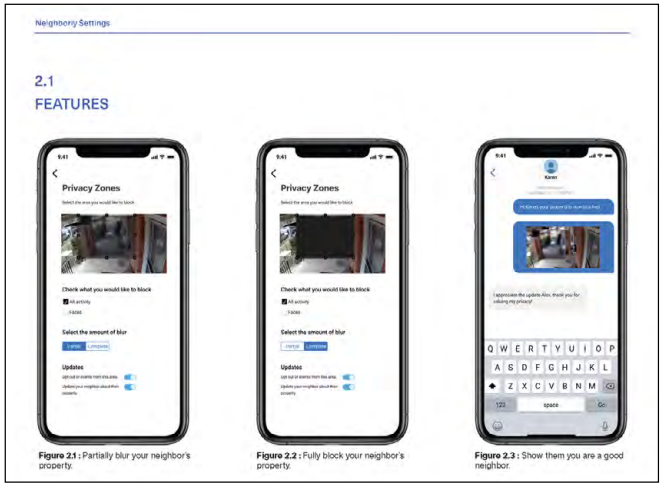
We created simplified versions of each of our top proposals to share with participants for concept evaluations, which we report on later. We conducted concept evaluations with two core goals: (1) To test whether the concepts were worth developing further with functional prototypes, and (2) to elicit responses to help us better understand the preferences and perspectives of primary users, adjacent actors, and various conflicts and cooperations between them.





Example detailed design proposal. *Neighborly Settings* is a feature that enables—and gently nudges— camera owners to be better neighbors by voluntarily blocking views of their neighbors' property, such as their yards, windows, and entryways. This design was inspired in part by the "activity zones" feature of current smart home cameras, which allow users to delineate areas, such as their porch, where they'd like to receive event alerts such as "package detected" or "unfamiliar face detected." Neighborly settings inverts this filter: users select areas to *not* get notifications and *not* record video to respect someone else's privacy. This feature is further inspired by text buried within the Nest Camera Privacy Guidelines that asks users to "Follow the golden rule" and "Treat others the way you'd like to be treated." From our prior empirical studies of smart cameras [33], we knew that some users use the activity zones feature to protect their neighbors privacy. Our Neighborly Settings feature is designed to nudge users to protect neighbors, and to shape new social norms through actionable features (as opposed to guidelines nobody actually reads [25,27,31]).





Example simplified design proposal. We significantly abbreviated each proposal to create a set of pages that were used during each concept evaluation interview.

Overview of Design Proposals

From our set of approximately 20 top design concepts, we developed 7 design proposals that we shared with participants. A summary of each proposal and a sample of the materials shown to participants is presented on this page and the prior page.

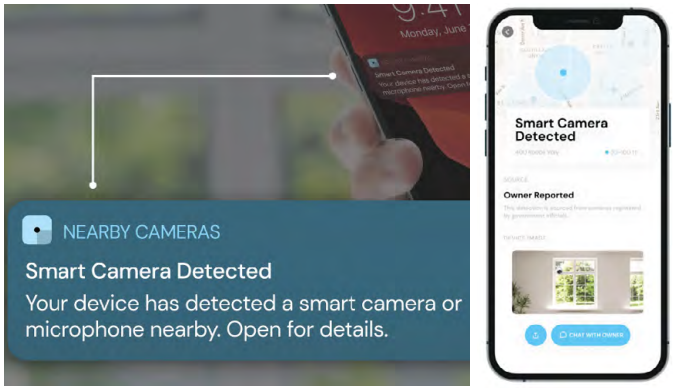
Downselection process. We further narrowed our work by excluding overly conceptual, poetic, or provocative concepts. We wanted participants to easily imagine our designs as everyday products or features, even if the technical implementations or economic incentives were quite speculative.

We developed two main criteria that helped us downselect concepts: (1) Does this seem like a potentially useful tool for primary users and/or adjacent actors? (2) Will this concept elicit reflection and discussion about privacy, trust, and adjacent actors?

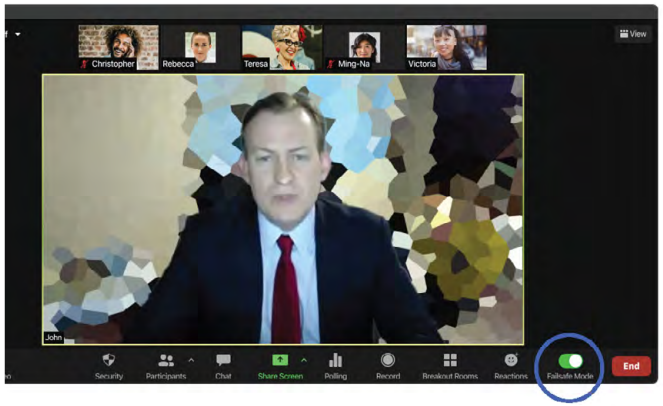
Closed Mode and Guest Access

In our expert view, our design proposals for *Closed Mode* and *Guest Access* represented the two most feasible concepts with high potential value to primary users and adjacent interactors. We deemed the remaining 5 design proposals more speculative with regard to implementation and value to users (similar to, for example, [4]). For example, our Nearby Cameras concept glosses over numerous legal, social, and technical hurdles. Yet it proved very useful in eliciting responses that helped us understand the concerns of primary users and adjacent interactors.

Whereas speculative design is often understood as provocative or frictional [30], we developed our designs with a philosophy of creating *subtly* speculative or frictional proposals. Next we elaborate on Closed Mode and Guest account in greater detail.

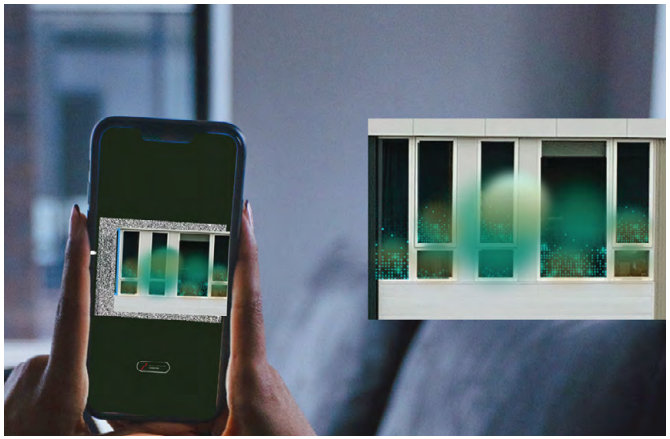


Nearby Cameras is an application that sends notifications when a nearby camera or microphone is detected. Types of cameras detected may include residential cameras, retail cameras, police cameras, and hidden cameras.



Webcam Failsafe Filters allow a user to automatically block distracting, embarrassing, or sensitive activity from entering into the frame of their video call. Users can block specific events such as yelling, people, or nudity.

Do Not Facetrack is a feature that allows people to require that their faces are automatically blurred on other people's security cameras.



Camera Shields is a device that users place in their window to block cameras from peering inside. It uses infrared LEDs to confuse sensors [25].

Closed Mode is set of privacy features integrated into a smart home camera that clearly communicates the status of the device to people nearby.
See pages 5–8.

Neighborly Settings help camera owners be better neighbors by blocking views they shouldn't monitor or see. *See page 3.*

Guest Access enables owners to give others partial access and control of their security cameras to improve guest's privacy, trust, and experience.
See pages 9–10.

Closed Mode

Closed mode is a cluster of privacy features that clearly communicates the sensing status of a smart camera to nearby actors, including camera owners, household members, visitors, and bystanders. Closed Mode is designed with indoor wired and battery powered smart cameras in mind, including those used to monitor pets, kids, guests, and domestic workers.

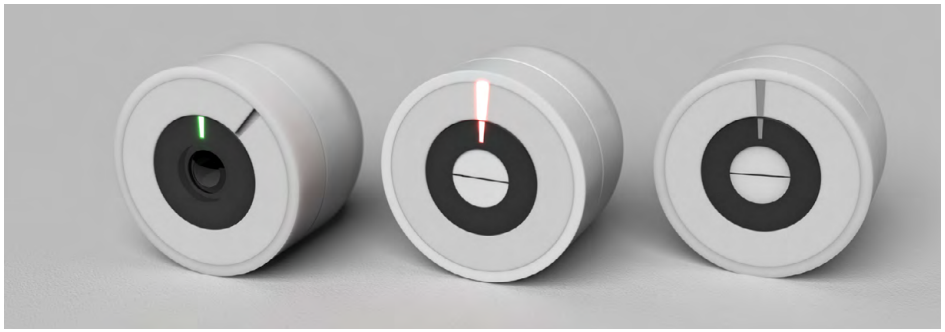
The central component is a pronounced *lenslid* that functions like remote controlled webcam cover. Visual and auditory indicators provide additional feedback. Together these components provides *tri-modal feedback* (visual, auditory, and physical/tactile movement indicators) that saliently communicates the camera status in an intuitive and transparent manner.

There are several ways of *controlling closed mode*: remotely via the app, physically by touching the device, and automatically by configuring *closing rules*.

Nanny notices camera appears on. Owner had said they should close camera it if on.

Nanny manually closes camera. Camera is now clearly off.

Owner receives a notification that camera was closed.



General Situations Addressed

Nearby actors cannot reliably know whether a smart camera is sensing or not just by looking at the device. Visual indicator lights may be unreliable [6,16]. Because smart cameras lack physical controls located on the device, it is also difficult to quickly and reliably enable or disable the camera.

Nearby actors affected by these issues include household members, short-term visitors, long-term guests, tenants, Airbnb guests, and tradespeople and domestic workers (nannies, babysitter, caregivers, house cleaners, pet sitters, carpenters, plumbers, delivery drivers, social workers).

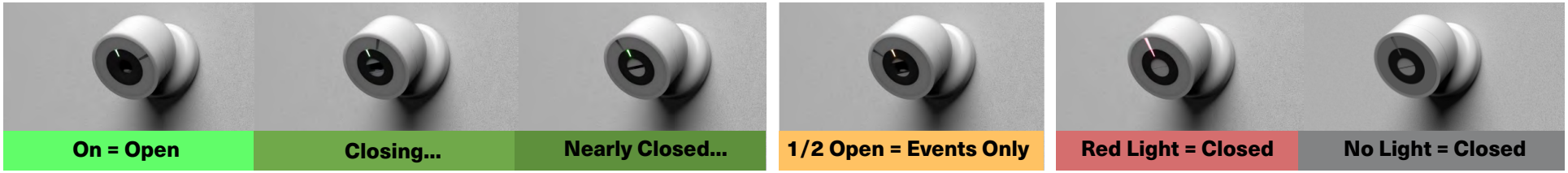
Example Use Case Scenarios

Closed mode is primarily designed for indoor smart home cameras. Closed Mode is useful in situations where owners sometimes want to be able to monitor specific areas of their home such as entryways, kids rooms, or areas where pets are active, but also want to reliably disable cameras when household members or guests desire privacy. Example use cases include:

Friend visiting. You like to keep the camera on during the day to watch your kids. A friend visits, and they eye the camera suspiciously. You open up the camera app, tap a button, and all of cameras visibly and audibly close, putting your friend at ease.

First person home. Your camera is on during the day to watch the dog, but no one wants it on while home. The Still Sensing feature (see page 8) chirps and blinks when it detects that a household member has arrived home. The first person home then remembers to turn off all the cameras.

Pet sitter. You're away for a few weeks and setup cameras to watch your pets. You've hired a pet sitter, but don't want to invade their privacy. You enable "Tap to Close" and tell the pet sitter they just need to gently tap the rim of the camera and the device will turn off completely. You can remotely open the camera again with the app after they leave. This way, you can also still see when the pet sitter arrived for work.



Tri-Modal Feedback: Trust Via Redundancy

The core idea motivating Closed Mode is to provide enhanced status indicators and reliable overrides. *Enhanced light indicators* and *auditory indicators* clearly communicate the camera status. The centerpiece feature is a *lenslid* shutter mechanism that physically closes to cover the camera lens, much like a webcam cover. This *tri-modal feedback* provides helpful redundancy, in case a nearby user doesn't notice one mode of feedback. The lenslid functions as a visible and intuitive override that provides an important layer of trust for guests or users who question the reliability of indicators. Together, these features aim to eliminate ambiguity, improve accessibility, and send a subtle signal that privacy and trust are paramount for owners, visitors, and bystanders alike.

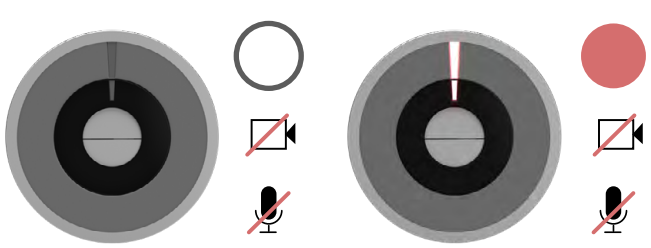
Electromechanical Lenslid

The *lenslid* is controlled by a small motor that protracts and retracts the shutters, similar to eyelids. The physical cover also provides latent tactile feedback. The user can touch the opaque plastic shutters to intuitively verify the camera lens is blocked, should they question the reliability of LED indicators and the honesty of camera owners or companies. The lenslid also includes an integrated visual indicator. When open, the lens appears dark. In Closed Mode, the protracted shutter displays a contrasting white. At a glance, the white shutter shows the camera is closed. The lenslid further serves as an accessible indicator to support color blind users. We are continuing to iterate on the design of feedback indicators and test variations with users.

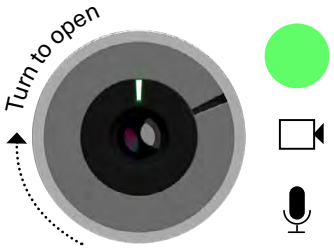
Light Indicators

Current smart cameras typically use small LEDs to show 3 main states: no lights = video/audio disabled, solid green light = video/audio enabled, pulsing green light = owner is live viewing video. Our camera employs more prominent light and sound indicators, and displays additional states.

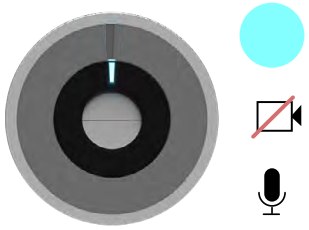
Our camera shows an additional state that some smart cameras offer: a battery-saving (and, in some contexts, tacitly privacy-enhancing) mode that intelligently monitors for user-specified events such as animals, smoke, or unfamiliar faces. Recordings and live view activate when an event is detected.



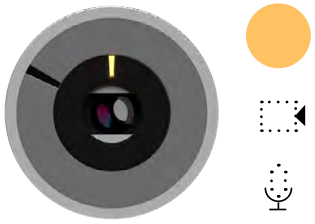
Closed State.
Camera and mic are deactivated.
White lenslid shutter confirms off status to adjacent actors.
Option 1: Red LED lit. **Option 2:** No LED (Red fades out)



Open State.
Camera is active.
Live and recorded video.
Green LED lit.



Mic Only State.
Video deactivated
But mic is sensing.
Blue LED lit.



Half Open State.
Event monitoring only.
No live or recorded video.
Orange LED lit. Slightly closed.

Auditory Indicators

Camera owners can configure up to three auditory indicator options: Tone, Basic Voice, and Advanced Voice. The volume of each can be adjusted independently. *Tone:* An ascending tone is played when Opening, and a descending tone is played while Closing. An oscillating tonal progression is played to indicate a Half Open State. *Basic Voice Indicators* provide an abbreviated description of changes in camera status, such as “Camera is now closed,” “Camera is now open,” and “Camera is now partially open.” *Advanced Voice Indicators* offer additional description of camera status for guests or bystanders unfamiliar with the device. For example, "The microphone has been turned on by guest user Sasha."

Closed Mode Basic Controls
There are 3 main ways to close or open the camera.

(1) Remote Control via App Interface.
Camera owners or invited guests can open and close the camera remotely via the app interface.

(2) Manually via Physical Device Control.
If enabled by the camera owner, a nearby user can touch the rim of the camera to close it. Camera owners can explain this hidden closing affordance to guests and household members.

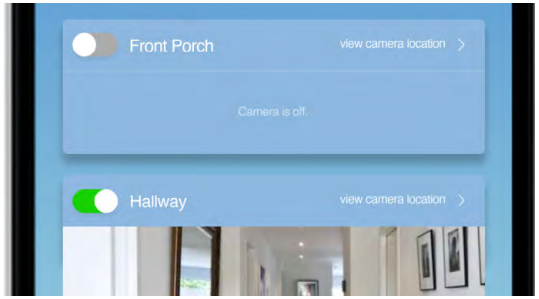
(3) Automatically via Intelligent Closing and Opening Rules.
Owners can configure advanced rules to automatically schedule or intelligently trigger opening and closing based on events. For example, users can configure cameras to close when a household members face is detected, close when nudity is detected, or open when smoke or breaking glass is detected.

Advanced Closing Rules and Situational Indicators
Several additional features allow even greater control.

(4) Repositioning Rules and Alerts
Cameras can be configured to close and/or notify users if moved or repositioned.

(4) No-Sense Zones
No-Sense Zones automatically activate closed mode when a camera enters an off-limits areas. Owners can configure geofenced No-Sense Zones around sensitive areas such as bedrooms, bathrooms, and guest rooms. This feature is especially useful for managing mobile battery-powered smart cameras. It may also be useful for integrated mobile (Group 2), autonomous (Group 3), and wearable (Group 4) cameras.

(6) Still Sensing Reminders
Even with lenslids and LEDs, people may still forgot or not realize that a camera is active. Still Sensing Reminders audibly chirp and visibly flicker to announce to those nearby that there's a live camera. For example, an owner may configure a camera to trigger a Still Sensing Reminder when a household member first arrives home. This can help household members remember to turn a camera off, and help guests or domestic workers locate cameras the owners have invited them to disable.

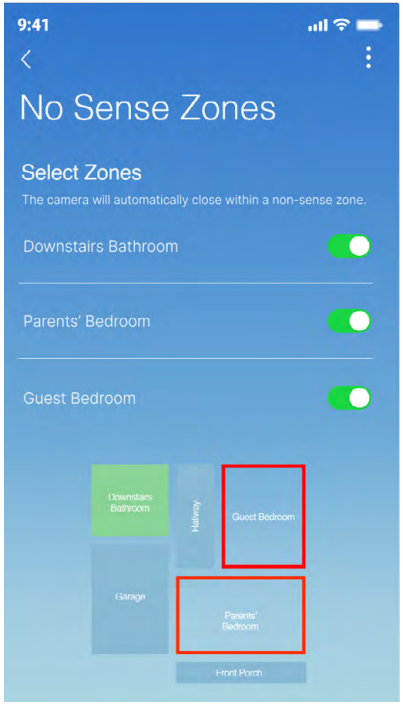


(1)

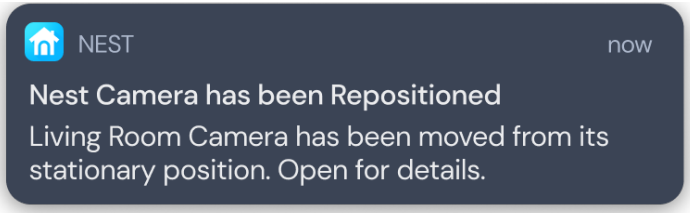

(2)

(3a)

(3b)



(5)



(4)

(6)

Guest Account: Goals and Rationale

Guest Account is a feature that enables owners to give limited access to their smart security cameras to improve a guest's privacy, trust, and relationship with the owner. Owners can share the specific location and status of their cameras with guests. The owner may also enable the guest to turn off certain cameras, or request a camera is disabled. Other features include enabling guests to opt-in to event notifications, such as "package seen," and an advanced feature that masks the guests face and voice from appearing on owner's app.

General Situations Addressed

Guests may feel uncomfortable or resentful about smart cameras in spaces they are sharing. But owners may not want to give them full co-user access. With nannies, caregivers, and Airbnb guests, owners may need to strike a delicate balance between maintaining a good relationship with guests while retaining the ability to review video if an incident occurs or they suspect a guest has done something inappropriate or illegal. Offering to provide guests with partial, temporary access may make guests feel more comfortable and respected—even if they do not actually setup the guest account. Similarly, the camera owner may feel better having offered to provide guest access, and use the feature as a way to introduce cameras to guests. Guests may find cameras less ominous once they have been granted and entrusted with partial access.

Example Use Case Scenarios

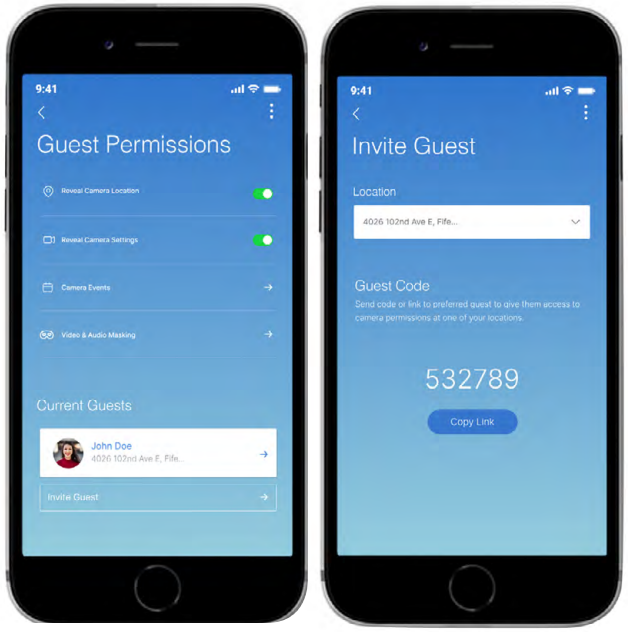
Below is a sample of several relavent use case scenarios we considered when designing Guest Account.

Nanny. You hire a nanny to watch your kids while you're at work. You also have several smart cameras to watch your kids, monitor pets and packages, and generally make you feel safer. You want your nanny to feel safe and respected. You give the nanny guest access so they know when the cameras are on. The nanny also uses them to monitor the front door. Guest access is enabled only during their working hours.

Airbnb Guest. You regularly rent your in-law unit on Airbnb. After a guest breaks the rules and throws a big party in your yard while you're away, you install a camera in the backyard and doorway to the unit. To help comply with Airbnb camera disclosure policies, and to make your guests feel respected, you give them limited guest access that expires when they checkout.

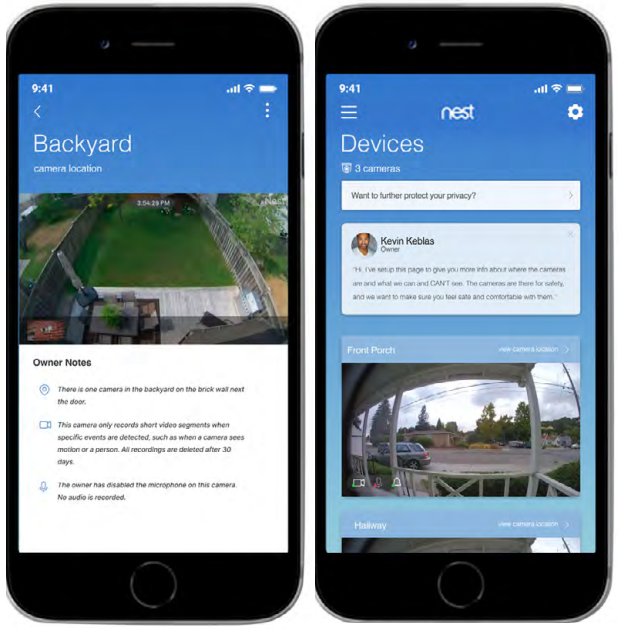
Live-in Friend. Your friend is going through a rough patch and is staying at your place for a few months. You give them guest access to your cameras, which allows them to receive notifications and turn the cameras off (although you can still override them).

Friend with keys. You let your friend use your apartment between their two jobs. Guest access lets them easily disable the smart cameras you use to watch your dogs.



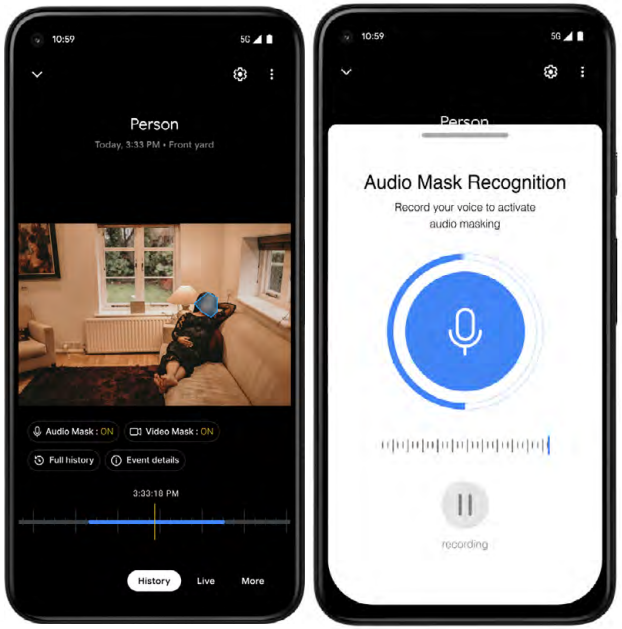
Owner Setup of Guest Permissions

The owner decides what features the guest can access, and when the guest account expires. The invited guest then decides which, if any, features to use.



Shared Camera Location and Status

Owners may share the location and status of the cameras to clarify precisely what the camera owner can and cannot see.

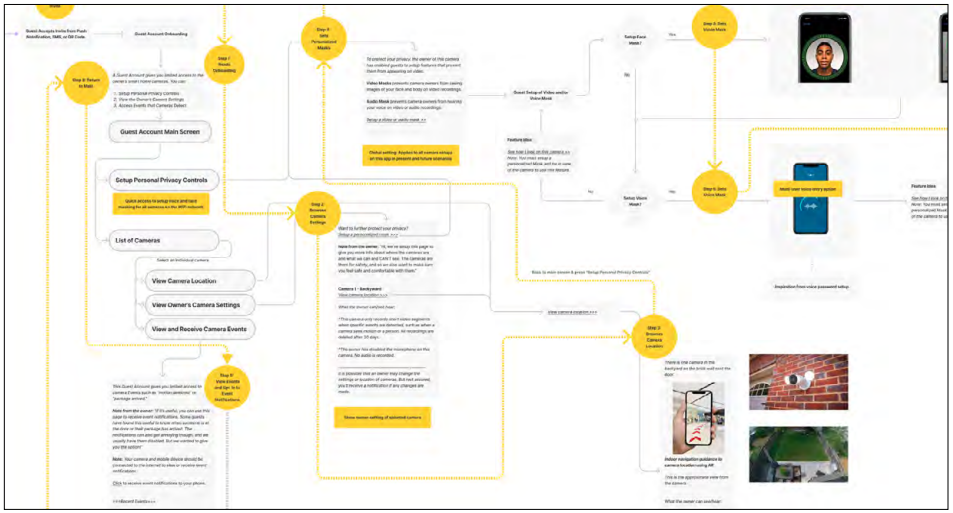


Video and Audio Masks

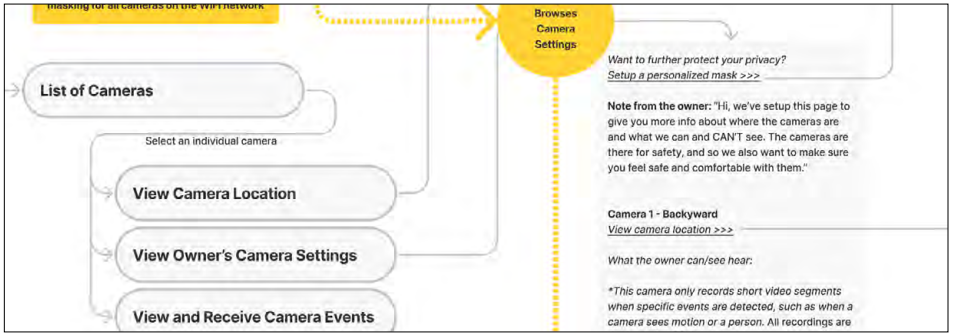
If enabled, guests can mask their faces, bodies, and voices from detection.

User Flows and App Architecture

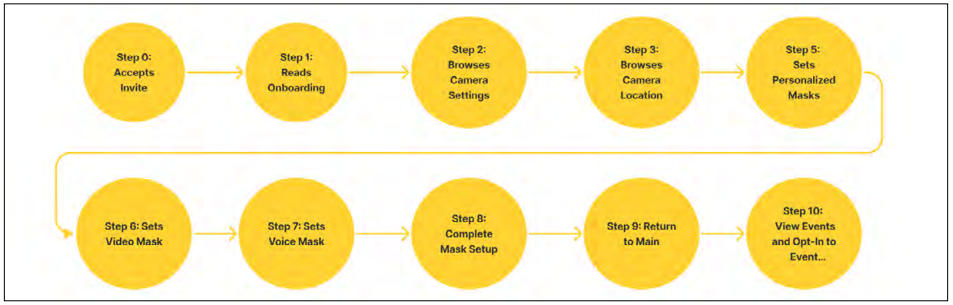
We created detailed user flows and information architecture for Guest Access. Flow diagrams show the steps users take to use an app and accomplish goals. Because detailed interaction flows are difficult to communicate concisely, below we highlight a few key features of our process, particularly our inclusion of non-ideal use cases.



A Guest Access flow diagram with a typical guest flow overlaid in yellow.



Details showing steps in typical guest user flow.



A simplified typical user flow for a Guest Access.

Idealistic Use Case (Simplified Storyboard)

Guests arrive and you give them the tour. You explain your cameras and offer them guest access.

You send them an invite, and they setup the account. They can now see where all cameras are located, and setup a few other features.

Other Use Case Examples: Imperfect, Nuanced, and Antagonistic

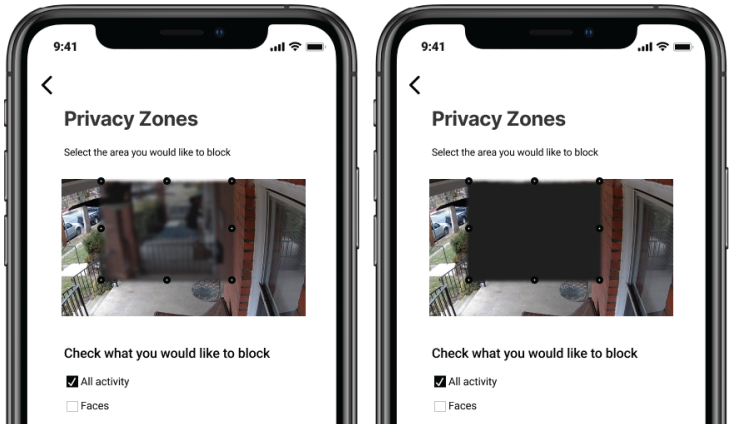
Alongside the typical idealized user flows, we created flows depicting more nuanced or less-than-ideal situations that might unfold with Guest Access. This allowed us to improve our design,while also considering how these features could fail or worsen situations. Below are several examples of atypical use cases for an Airbnb rental.

Broken Trust. An Airbnb guest is granted Guest Access. The guest later exceeds the max allowed guests, breaking the hosts Airbnb policy. After the guest repeatedly breaks the rules, the host unmasks video footage and sends the video to the guests, proving they violated the policy.

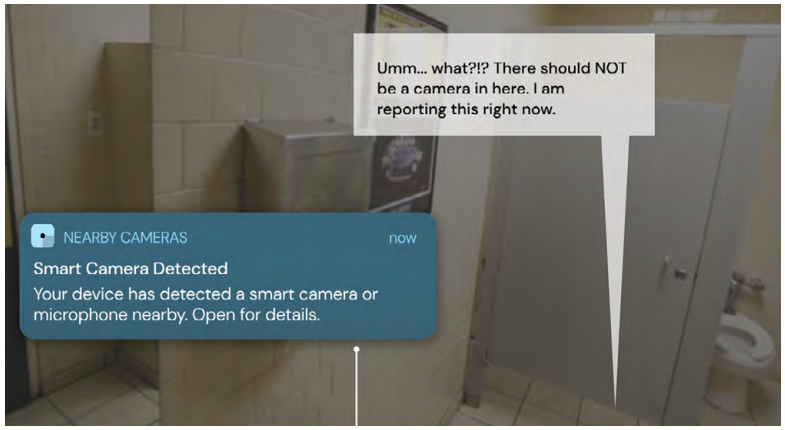
Full Reversal. An Airbnb guest is very skeptical of the host's cameras at first. But after using Guest Access, they quickly find the notification annoying and irrelevant. They become desensitized to the cameras, and stop caring what the owner sees. They realize just how boring and innocuous the camera recordings are. Guest Access effectively defanged the cameras for this guest.

Keep it down, please. An Airbnb guest is planning a party, which they know is not allowed. They check the camera status and patio cameras and mics are disabled. But they host receives a smart sensing notification that decibel levels are excessive. They enable the mic. As promised, the guest receives an automatic notification that the owner has changed a cameras status. But they're drunk and miss the notification. Later, the Airbnb guest receives an "excessive noise" message from the host. They are a little annoyed, but quiet down before the host has to resort to calling them.

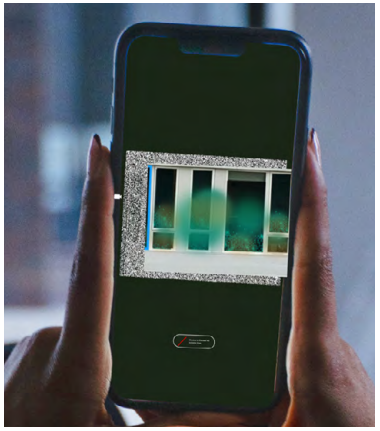
No one is that nice. Guest Access is still a new feature, and some Airbnb guests find it very strange. Why are hosts willing to share access with them? Do they have other hidden cameras they're trying to cover up by pretending to be transparent?



Tensions exposed with Neighborly Settings. "*I prefer blur over block because I can see what's happening. ... But I do want to protect my neighbor's privacy*" (P6). Curiosity piqued by Nearby Cameras. "*I would 100% be interested in downloading this app ... Like, what is happening?*" (P2).



Nearby Cameras: Helpful, depending on situation. *"It'd be helpful to know if there's a hidden camera in my Airbnb. But for other scenarios, we're on cameras so much already while entering a store and so on - you kind of leave the house with this in mind. Though it'd be great to be able to give consent before being filmed*" (P4).



Camera Shields: Empowering the surveilled subject. *"This is a great concept because you can actively do something if you feel your privacy is being violated" (P1).*

Concept Evaluation User Study

We conducted concept evaluations of our 7 designs with 11 participants. We recruited participants with a variety of experiences as camera owners, guests, bystanders, domestic workers, and subjects of surveillance. For example, participants included 1 professional pet sitter, 1 frequent Airbnb guest, 1 frequent house-sitter, 1 caregiver of other people's children, and 1 person whose roommate owned smart cameras they lacked access to. Following an introductory discussion, we showed participants documentation for each of the concepts (see page 4) and facilitated conversation using a semi-structured discussion guide (*see supplemental documentation*). We selectively transcribed interviews and used a modified grounded theory process to code emergent themes. We present a selection of preliminary findings from these interviews, focusing on responses to Closed Mode and Guest Access.

Closed Mode

All participants identified situations where Closed Mode would be useful for them personally. The most commonly cited use was protecting the privacy of guests. For example, P1 imagined using Closed Mode when guests were over for a backyard barbecue. P5 went even further by discussing how Closed Mode could help camera owners do the right thing and disclose the status of their cameras to people nearby: "As an owner you should give other people a peace of mind by normalizing conversations about it and let people know if they are being recorded or not" (P5).

Providing peace of mind for household members was a commonly cited motivation for adopting Closed Mode. For example, one participant described a workaround where they would turn their living room smart camera toward the wall after they had switched it off to provide an extra layer of protection. They described a significant tension between their desire for home safety and security, which their smart security cameras provided, and concerns that their own camera might invade their personal privacy, either through disclosure to another household member or to the product's manufacturer. "I don't like the aspect of being watched from the camera while being at home ... I wish there would be something to completely turn it off [other than unplugging it]" (P2).

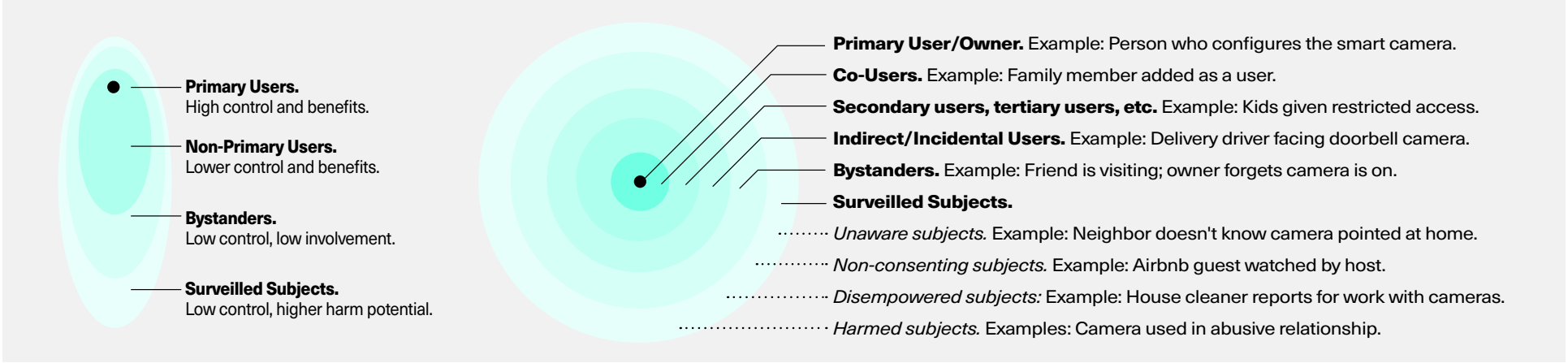
All participants found the lenslid mechanisms to be a reliable and intuitive way of assuring themselves, household members, and guests that the camera sensor was effectively disabled. Some participants further discussed how Closed Mode offered a valuable assurance because they did not trust the built-in indicator lights. "I don't trust the light as the only indicator to communicate if the camera is recording or not." (P3); "A friend of my step dad installs cameras at people's homes and told how he can manipulate the physical indicator whether the camera is working or not" (P4).

One limitation is that Closed Mode does not address audio recordings as well as video because it does not offer a reliable and intuitive mechanism for disabling microphones. For some participants audio was experienced as a more significant threat to privacy than video: "Most private stuff happens in conversions rather than image" (P1).

Two participants suggested that in some situations Closed Mode might draw too much attention to their device. P6 described a complicated situation where she was using smart cameras to monitor a landlord who was showing her home to prospective buyers. P5 described a desire to minimize the prominence of his smart cameras within his home, rather than calling attention to them because he feels uncomfortable when he has to explain them to guests. He prefers smart devices "do not dominate" his home.

Guest Access

All of our participants liked the idea of sharing access to their smart home cameras with guests. Participants envisioned themselves sharing guest access across many of



our anticipated scenarios, including long-term house guests, sublettors, house sitters, and Airbnb guests. Participants generally felt comfortable sharing access with these guests. As one participant said, “You already trust the person enough to be in your place so why not give them access to your smart cameras!” (P3).

Our design of Guest Access considered a general use case where a camera owner offered a guest access and they declined, yet the feature still succeeded in making the guest and host feel more comfortable with the camera and one another. In this scenario, guest access functions like a peace offering or tacit contract. Several participants recognized this opportunity without us first highlighting it. For example, P6 said she might offer guest access to her mother in-law when she comes to visit. “I don’t know if she’d use it, but I like the idea that she’d feel in control of her privacy.” One potential concern with Guest Account was ensuring that this access expired after the guest’s stay, especially if more substantial privileges were granted such as the ability to disable a camera.

Conclusion: Key Contributions and Future Work

Exposing adjacent actor privacy. Spatial sensing technologies, particularly cameras and microphones, affect the privacy of people nearby. In these situations, "the user" as a generic catchall term needs to be expanded and nuanced. In contexts involving spatial sensing devices or surveillance, the concept of "the user" belies a more diverse range of roles along a spectrum from primary device user/owner to surveilled subject. In the diagrams above, we summarize a tentative vocabulary for addressing adjacent actors. Instead of assuming the mantra that good design means improving "the user experience," our design situations foreground the question of whose user experience should be prioritized when there are many users and (inter)actors involved, each with varying degrees of control, access, and consent, not to mention competing goals and interests.

Mapping a design space, and showing our work. Too often, research through design publications focus on design outcomes and empirical findings to the neglect of intermediate knowledge artifacts and key landmarks within the design process [11,18]. This is unfortunate to the extent that these outcomes may be valuable to others working on related topics or similar challenges. Here we have presented several analytical frameworks describing design considerations for smart cameras. We have also demonstrated ways of adapting the design methods of scenarios and use cases to elucidate adjacent actor needs and preferences alongside those of primary users, and to surface tensions and competing interests between them.

Detailed and partially validated design interventions. Our concept evaluation study was roughly one half exploratory and one half evaluative. Overall our study provided strong validation for Guest Access and Closed Mode, and we plan to continue designing and prototyping these systems. We further found our remaining proposals were effective prompts for understanding people's privacy perceptions and preferences.

Our design proposals form an important contribution addressing a key gap in the design landscape. While prior work has foregrounded the need to address adjacent actor privacy with smart sensing devices [e.g., 24,36,29] , few concrete and detailed design interventions have been proposed to address these issues specifically [for examples, see 5,8,9,23,26,28,33]. We find three key reasons for this. First, there is a lack of incentives for companies to address the privacy of people who are not their direct customers. Second, many conflicting incentives exist among primary users and adjacent actors. Third, even when cooperation and shared incentives do exist, there are many challenges to offering controls that can be reliably shared and verified by relevant stakeholders.

Identifying limits of interfaces, technologies, and individuals. While our scenarios and design interventions challenge the prevailing notion of "the user," at the same time our work consciously stays very close to other conventions within HCI and interactive design, including the focus technological interfaces and individual controls as a point of intervention. A design approach instead focused on collective and structural interventions, such as platforms or policies [e.g., 13,20,22,32,35], would likely yield other outcomes. While our work identifies potential design solutions, our inquiry also exposes limitations and challenges. Individual devices and controls are clearly insufficient for addressing the broader array of privacy, security, and trust issues that entangle primary users, adjacent actors, and sensing devices. As is often the case with vexing and murky design challenges, more work is clearly needed.

Conclusion: Key Contributions and Future Work

We thank Daniela Rosner, Audrey Desjardins, Yuna Shin, Chandler Simon, Gabrielle Benabdallah, Stephanie Waldrop, and the anonymous reviewers for their feedback on this work. We also thank the participants in our study for sharing their feedback and perspectives. This work was supported in part by the National Science Foundation (NSF) under grants "CHS: Multidisciplinary Approaches to Privacy and Security" (#1910218) and "CAREER: Designing Human-Centered Privacy, Security, and Data Ethics for Non-Primary Smart Device Users" (#2142795), and by the Center for Long-Term Cybersecurity (CLTC) project grant " "Cybersecurity for Non-Primary and Primary Users of Always- On Internet of Things Devices." Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF or CLTC.

References

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

2. Arne Berger, William Odom, Michael Storz, Andreas Bischof, Albrecht Kurze, and Eva Hornecker. 2019. The Inflatable Cat: Idiosyncratic Ideation of Smart Objects for the Home. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 401, 1–12. https://doi.org/10.1145/3290605.3300631

3. Julia Bernd, Ruba Abu-Salma, Junghyun Choy, and Alisa Frik. 2022. Balancing Power Dynamics in Smart Homes: Nannies' Perspectives on How Cameras Reflect and Affect Relationships. Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS '22). To appear.

4. Nico Brand, William Odom, and Samuel Barnett. 2021. A Design Inquiry into Introspective AI: Surfacing Opportunities, Issues, and Paradoxes. In Designing Interactive Systems Conference 2021 (DIS '21). Association for Computing Machinery, New York, NY, USA, 1603–1618. https://doi.org/10.1145/3461778.3462000

5. Finn Brunton and Helen Nissenbaum. (2015). Obfuscation: A user's guide for privacy and protest. MIT Press.

6. John Carroll, Duffy, T. M., Osgood, D., Holyoak, D., & Monson, D. (1996). Scenario-based design: envisioning work and technology in system development. IEEE Transactions on Professional Communications, 39(4), 241-241.

7. George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 555, 1–16. https://doi.org/10.1145/3411764.3445691

8. Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376304

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

10. Nazli Cila, Iskander Smit, Elisa Giaccardi, and Ben Kröse. 2017. Products as Agents: Metaphors for Designing the Products of the IoT Age. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). Association for Computing Machinery, New York, NY, USA, 448–459. https://doi.org/10.1145/3025453.3025797

11. Audrey Desjardins and Cayla Key. 2020. Parallels, Tangents, and Loops: Reflections on the 'Through' Part of RtD. Proceedings of the 2020 ACM Designing Interactive Systems Conference. Association for Computing Machinery, New York, NY, USA, 2133–2147. https://doi.org/10.1145/3357236.3395586

12. Nils Ehrenberg and Turkka Keinonen. 2021. The Technology Is Enemy for Me at the Moment: How Smart Home Technologies Assert Control Beyond Intent. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 407, 1–11. https://doi.org/10.1145/3411764.3445058

13. Casey Fiesler, Jeff Hancock, Amy Bruckman, Michael Muller, Cosmin Munteanu, and Melissa Densmore. 2018. Research Ethics for HCI: A Roundtable Discussion. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18). Association for Computing Machinery, New York, NY, USA, Paper panel05, 1–5. https://doi.org/10.1145/3170427.3186321

14. 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 (CHI '18). Association for Computing Machinery, New York, NY, USA, Paper 667, 1–13. https://doi.org/10.1145/3173574.3174241

15. 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) (pp. 21-40).

16. Adam Harvey. “CV Dazzle: Camouflage from Face Detection.” Accessed May 2, 2020. https://cvdazzle.com/

17. Ohad Inbar and Noam Tractinsky. "FEATURE The incidental user." interactions 16.4 (2009): 56-59.

18. Nadine Jarvis, David Cameron, and Andy Boucher. 2012. Attention to detail: annotations of a design process. In Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design (NordiCHI '12). Association for Computing Machinery, New York, NY, USA, 11–20. https://doi.org/10.1145/2399016.2399019

19. Tom Jenkins. 2017. Living Apart, Together: Cohousing as a Site for ICT Design. In Proceedings of the 2017 Conference on Designing Interactive Systems (DIS '17). Association for Computing Machinery, New York, NY, USA, 1039–1051. https://doi.org/10.1145/3064663.3064751

20. Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '04). Association for Computing Machinery, New York, NY, USA, 471–478. https://doi.org/10.1145/985692.985752

21. Bran Knowles, Sophie Beck, Joe Finney, James Devine, and Joseph Lindley. 2019. A Scenario-Based Methodology for Exploring Risks: Children and Programmable IoT. In Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19). Association for Computing Machinery, New York, NY, USA, 751–761. https://doi.org/10.1145/3322276.3322315

22. 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 (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 439, 1–13. https://doi.org/10.1145/3290605.3300669

23. 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, Article 102 (November 2018), 31 pages. https://doi.org/10.1145/3274371

24. Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. "Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts." Proc. Priv. Enhancing Technol. 2020.2 (2020): 436-458.

25. Kirsten Martin. "Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online." The Journal of Legal Studies 45.S2 (2016): S191-S215.

26. Gary T. Marx. "A Tack in the Shoe: Neutralizing and Resisting." Journal of social issues 59.2 (2003): 369-390.

27. Aleecia M. McDonald, and Lorrie Faith Cranor. "The cost of reading privacy policies." Isjlp 4 (2008): 543.

28. 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. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 5197–5207. https://doi.org/10.1145/3025453.3025735

29. James Pierce. "Smart home security cameras and shifting lines of creepiness: A design-led inquiry." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019.

30. James Pierce. 2021. In Tension with Progression: Grasping the Frictional Tendencies of Speculative, Critical, and other Alternative Designs. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 617, 1–19. https://doi.org/10.1145/3411764.3445406

31. James Pierce, Sarah Fox, Nick Merrill, Richmond Wong, and Carl DiSalvo. 2018. An Interface without A User: An Exploratory Design Study of Online Privacy Policies and Digital Legalese. In Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18). Association for Computing Machinery, New York, NY, USA, 1345–1358. https://doi.org/10.1145/3196709.3196818

32. 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 (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 84, 1–15. https://doi.org/10.1145/3290605.3300314

33. 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). Association for Computing Machinery, New York, NY, USA, Article 617, 1–25. https://doi.org/10.1145/3491102.3517617

34. Khai N. Truong, Shwetak N. Patel, Jay W. Summet, and Gregory D. Abowd. "Preventing camera recording by designing a capture-resistant environment." In

International conference on ubiquitous computing, pp. 73-86. Springer, Berlin, Heidelberg, 2005.

35. 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, Paper 262, 1–17. https://doi.org/10.1145/3290605.3300492

36. 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, Article 59 (November 2019), 24 pages. https://doi.org/10.1145/3359161

37. Eric Zeng, Shrirang Mare, and Franziska Roesner. "End user security and privacy concerns with smart homes." Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). 2017.

38. Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. Proc. ACM Hum.-Comput. Interact. 2, CSCW, Article 200 (November 2018), 20 pages. https://doi.org/10.1145/3274469