

Arca: Prototyping Design Patterns for Adjacent User Trust, Control, and Privacy with Smart Cameras

✕ Authors

James Pierce, Claire Weizenegger, Robyn Anderson, Hope Terpilowski, Wyatt Olson, Lian Bensaadon, Ann Lai, Faith Ong, Burke Smithers, Cobi Stancik, Cole Young

University of Washington, Seattle, USA

✕ Abstract

Companies and smart product designers prioritize the needs of primary users. However, smart devices with spatial sensors, like cameras and microphones, impact the experiences of people nearby. We refer to these people as adjacent users. We present a research through design project that highlights an overlooked need to design for adjacent users. This research outlines a range of actionable pathways forward in the form of design patterns, principles, and novel problem-framings. We also reflect upon barriers and inherent limits to user-centered design approaches. Our vehicle for generating and communicating these insights is a design concept and prototype called Arca. Presented as a fictional product, we brand Arca as “more inclusive, privacy-enhancing smart camera for you and your extended household.”

✕ Introduction

Current smart home devices understandably prioritize the needs of a primary user. This user is typically the purchaser and owner of the device and any corresponding software service subscriptions. Yet smart home devices with cameras, microphones, location tracking, and other spatial sensing capabilities invariably impact the experiences of people nearby—such as family, friends, guests, tenants, neighbors, domestic workers, and public bystanders. We refer to these individuals as adjacent users (or adjacent subjects). These users may interact with smart devices but often do so with little awareness, consent, access, control, or benefit.

Smart home cameras—such as Amazon Ring or Google Nest—are widely used across North America. While intended to deter intruders, monitor activity, and detect deliveries, these devices also provoke privacy concerns and interpersonal tensions between primary and adjacent users. This is especially true in cases involving visitors, domestic workers, or neighbors.

A novel element of these devices is their cloud-based subscription services, which unlock advanced features—like event detection, facial recognition, or sound alerts—powered by AI and cloud computing. These systems notify users when a known face appears, an animal is seen, or a sound is detected.

Consumer smart home cameras thus

represent an ideal site for investigating how design can address adjacent user needs. Research on bystander [6,44], non-primary user [23,46], and adjacent user privacy [41] and power dynamics [35] has emerged in response to these issues. Through empirical findings and critical insights, this research has successfully drawn attention to previously neglected power and privacy conflicts among primary users, adjacent users, and backend actors like companies and hackers. Yet design responses have not kept pace.

Several core challenges make resolving these tensions difficult:

- **Sensor spill out over space.** Sensor fields are invisible and extend into shared physical space.
- **Conflicting needs.** Primary users often prioritize security; adjacent users prioritize privacy.
- **Power imbalance.** Adjacent users rarely have access device interfaces or privacy settings.
- **Market incentives.** Companies design primarily for paying customers, not adjacent users.

To address these challenges, we conducted a two-year design research inquiry with two main goals: (1) design actionable improvements for both primary and adjacent user experiences with smart cameras, and (2) generalize insights through patterns, principles, and problem framings.

Our work culminated in Arca—a design

prototype that reimagines the smart camera. While Arca is a product concept for a more transparent and trustworthy device, it is also a research tool and public prototype that investigates systemic issues. Unlike conventional design, which ends with a product, research through design (RtD) aims to create knowledge [20,38,45] through conceptually generative artifacts.

This project distills design patterns [1,43], principles, and issues to grapple with privacy, power, and social dynamics—highlighting where traditional human-centered design falls short.

In conclusion, we summarize knowledge generated through our design process. We also reflect on design research artifacts generally, and our engagement with Arca as multi-functional artifact that we use for

- **anticipating futures**, including a future with many more sensors and invasive forms of surveillance,
- **imagining alternatives** such as new policies and standards requiring features similar to Arca's,
- **probing limits** of user-centered and interaction design, and
- **engaging others** with concerns and questions about privacy, power, and smart products.

Our approach builds on privacy scholarship in human-computer interaction (HCI) and science and technology studies (STS), drawing on Nissenbaum's



theory of contextual integrity [48] and Palen and Dourish's notion of boundary negotiation [37], which conceptualizes privacy as a dynamic process. Rather than a fixed state, privacy is understood as an ongoing, relational negotiation shaped by evolving social and technological contexts—particularly in interactions between primary and adjacent users.

A Note on Documenting *Product*

While research through design often emphasizes process, this Pictorial foregrounds product. We focus on the final design artifact—Arca—and the generalized design knowledge it offers. Due to space limitations, we omit many important empirical and process details but argue that exemplary design documentation is an important and often underappreciated research contribution.

✕ Primary and adjacent users

Digital privacy and surveillance discourse tends to focus on relationships between individuals (users, customers, subjects) and powerful, surveillant organizations such as companies, third-party advertisers, governments, and cyberstalkers [18]. This has been referred to as the vertical dimension of privacy [3]. Vertically, there is a significant power imbalance owing in part to a structural relation where the surveilling organization is some combination of (1) hidden “behind the scenes” (e.g., a third party advertiser or cybercriminal) and (2) in a position of extreme, unsalable authority (e.g., the corporate online service provider or a government agency with a subpoena).

The emerging discourse around “bystander privacy” foregrounds an or-

thogonal dimension we refer to as horizontal privacy. This involves interpersonal, and often face-to-face relations between “uneven peers” such as family members, friends, children, guests, neighbors, landlords, tenants, and domestic workers including nannies, caregivers, and pet sitters. Horizontal relations often entail power imbalances, such as between a parent and child, employer and nanny, or landlord and tenant. However, these relationships are interpersonal and often involve some level of pre-existing trust, respect, cooperation, and social exchange.

✕ Formative Prior Research

These findings are based on a two-year design research study, including over 60 interviews with both primary

and adjacent users of smart cameras. Our primary studies are informed by growing body of related work on bystander and adjacent user privacy [2,6,9,30,32,41,47,50,51,51]. Adjacent users—such as guests, neighbors, and domestic workers—often described feeling surveilled without consent or control, leading to interpersonal tensions, ambivalence, and quiet acceptance. Surveillance frequently reflected deeper issues of trust, autonomy, and respect. These dynamics underly key findings from our primary research with primary and adjacent users in our research.

Casual and incidental surveillance. Smart cameras encourage and teach primary users to surveil others, including in ways that primary users never intended. For example, features like event notifications prompt users to casually spy on neighbors and household members out of curiosity.

Silent disclosure and consent. Camera owners rarely disclose their cameras directly, but assume people will notice them. People do notice them, but rarely feel empowered to question, complain, or express their discomfort.

Interpersonal tensions. Surveilling people in their home and neighborhood can lead to resentment and indignation. Many adjacent users, like nannies and neighbors, feel disrespected and disempowered when they are surveilled. They often feel this way even though that have little or no concerns about the disclosure of their personally sensitive information, such as the content of video depicting how they are behaving.

Resistance and coping tactics. Adjacent users described creative ways that they use their relatively limited power and control to improve their experience, including avoiding spaces with sensors, overriding capabilities

(unplugging, covering, or repositioning devices), and attempting to communicate with primary users through cameras (e.g., waving or making faces at a neighbors’ cameras).

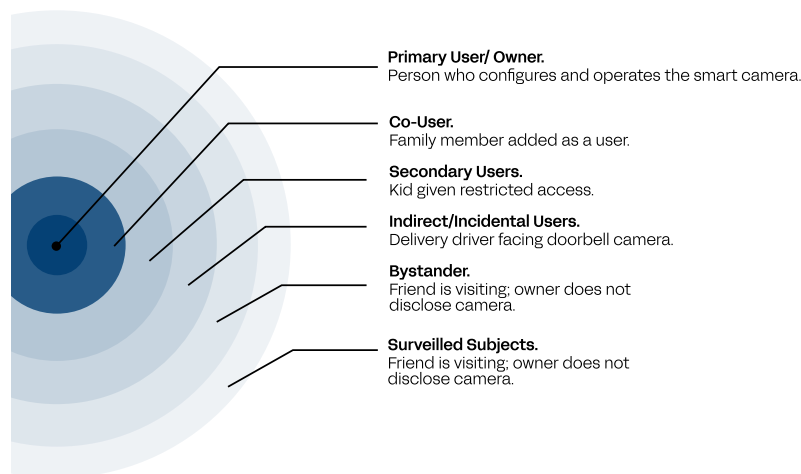
Ambivalence. We find many examples of ambivalence, coping strategies, and even acceptance of everyday surveillance by adjacent users—including self-regulating behaviors that have long been a concern of surveillance scholars. We find that smart camera surveillance has, at least in the home and neighborhood contexts of large US cities that we studied, become a normal aspect of daily life for many. This normalization further entails new social norms and expectations, such as our reported phenomena of silent disclosure and consent wherein primary users do not directly disclose cameras, and adjacent users notice. These insights directly shaped the design of Arca and our approach to addressing adjacent user needs.

This work contributes to the emerging body of privacy research within HCI and design [37, 48] by foregrounding design tensions in shared environments.

✕ Design Goals and Approach

Our user research and design analysis led us to synthesize five initial design principles:

1. **Extend power.** We aim to empower and encourage primary users to extend greater awareness, consent, access, control and benefit to adjacent users, as appropriate and dependent on context. We thus hope to help redefine social norms and expectations. Primary users hold most of the power and control; we aim to encourage them to share and disclose it.
2. **Discourage harm.** We aim to discourage incidental and casual surveillance. While we hope to prevent the most egregious forms of surveillance—such as non-consensual hidden cameras—the reality is that the worst actors will still find a way to act badly. We focus on inhibiting and dissuading primary users who can be nudged toward respecting the privacy and autonomy of others.
3. **Facilitate respect.** We prioritize the design of systems that improve respect, trust, and communication rather than fixating on protecting personal information. We aim to facilitate direct, open, and ongoing disclosure and consent.
4. **Nuance system states.** We seek to define and prototype privacy-enhancing states for sensing, processing, and displaying data. These states can help primary users manage and prevent situations of oversensing, overextracting, and oversharing of sensitive information.
5. **Systemically indicate.** We design indication systems that consider the different and sometimes competing needs and desires of various users—both primary and adjacent. Throughout our design process we consider the interplay between feedback provided by in-app indicators and on-device indicators. We also rethink the single LED point light as the ubiquitous default form of on-device indication.



Diagramming adjacent users. We can conceptualize adjacent users as radiating outward from a central primary user. At the out margins lie surveilled subjects who hold little or not awareness, consent, control, and benefit.

Overview

We begin with an overview of our design prototype, Arca—a fictional consumer product developed to communicate our ideas to broader audiences. These design choices were informed by interview findings highlighting concerns about ambiguous indicators, unwanted monitoring, and limited awareness and recourse.

Flexible Sharing. Arca encourages primary users to share access to their camera by offering several predefined levels of access. These ranges from equal Co-User to a limited Status View designed to inform neighbors or guests but without allowing sensitive access to audio, video, or controls.

True On/Off Indicators. Arca clearly communicates when the camera and microphone are recording, and when they are fully disabled.

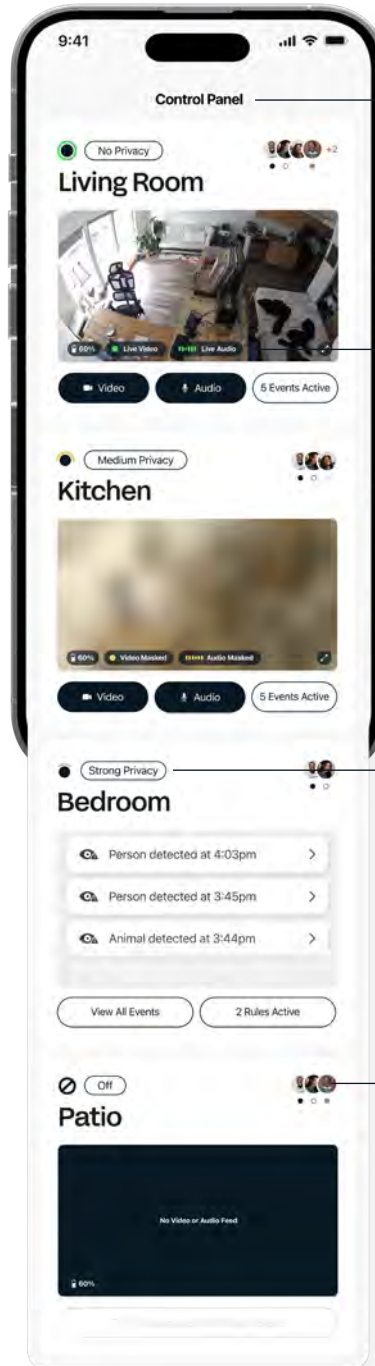
Medium Privacy Mode masks video and audio by default, but allows owners to unmask the video if needed. Medium privacy adds various forms of friction that inhibit users from frivolously spying on others.

Strong Privacy Mode completely disables video and audio, but allows users to stay informed with text summaries of events—such as “cat seen” or “unfamiliar face detected.”

Privacy Zones allow users to apply Medium Privacy, Strong Privacy, or True Off to a portion of the camera’s field of view—such as a neighbor’s property.

Rules enable custom automated mode switching triggered by Events. For example, parents can program their indoor cameras to switch from Medium Privacy to True Off when their kids arrive home from school.

Sensor Overlay Indicators physically cover the camera lens in Medium Privacy, Strong Privacy, and True Off modes. The lens covers block or tint the video. This has functional and symbolic value with regards to trust and transparency.



Control Panel: Provides consolidated access to the most important buttons and indicators. Current smart camera apps require multiple taps to perform basic tasks like turning the camera off.

Audio Indicators: Visually communicates if the microphone is activated or deactivated.

Live Audio

Privacy Modes Selection: The most novel feature of our product, Privacy Modes allow users select sensing and recording states between “fully on” and “fully off.”

Shared Access Indicator & Settings Bar: Clearly shows if access is shared, and with how many users.



Video figure: The short version of our fictional promo video showcases some of Arca’s key features.

Indication System

States between On and Off

Arca employs a novel dimmer switch analogy, allowing users to adjust the camera's sensors to achieve the right balance of privacy and security. Whereas most smart cameras indicate two basic modes (on or off), Arca indicates a discrete spectrum of four states: True On, Medium Privacy, Strong Privacy, and True Off.

It took many iterations of design and user testing to settle upon the number, name, and functionality of these basic privacy states. We found that more than four states tended to impede recall and learnability. We also found that the “circle and dot” layout pattern was an economical, flexible indicator pattern for communicating a range of privacy states on space-constrained devices.

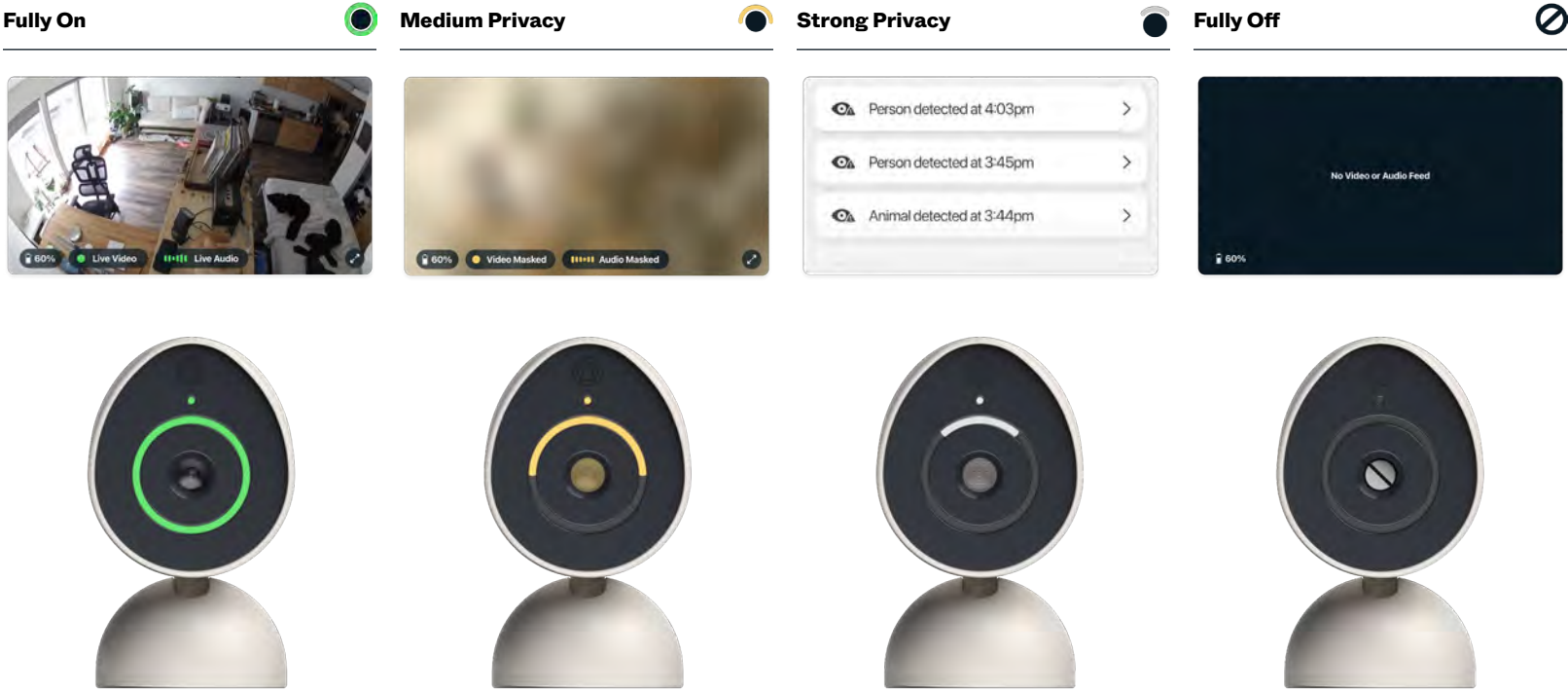
A major insight of our design is to communicate a spectrum of privacy states through on-device indicators that are accessible to both primary and adjacent users.

Open and Closed Metaphor

Instead of a binary “on/off” indicator using a single point light, our indication system suggests a continuum from “open” to “closed.” A fuller indicator represents a more powerful (and more privacy-invasive) state. A diminished indicator represents a less powerful (and less privacy-invasive) state. Lindley et al explore similar metaphors [45].

Tri-Modal Indication System

Our design maximizes communicative potential from limited display real estate. We achieve this with unconventional layout patterns for point-light LEDs, supplemental sound indication, and an electromechanical lens cover.



Accessibility. To accommodate color deficient and low vision users, size and shape are the primary indication attributes; color is a redundant attribute.

Sensor Overlay: An electromechanical lens cover system is implemented with linear actuators. Functionally, the covers block or tint light entering into the lens. Symbolically, they convey extra layers of trust with a physical layer of material. Our innovation extends automated web covers [e.g., 8] by introducing multi-state covers with tint and texture.

High and Low Visibility Settings: If discretion is desired, users can select a Low Visibility mode. Brightness can be adjusted from ultra-bright to very dim. But to maintain trust through reliability, it is not possible to completely disable the indicator lights.



✕ Updating the Basic On/Off

Differentiating “on” and “off” states is straightforward with simple electrical devices. But digital devices with sensors, network connectivity, and data processing capabilities contain a multitude of ons and offs. The various sensors, processors, and actuators of these systems regularly permute through countless states of digital on/off, true/false, and 0/1. Given the trend toward “always on” devices, the concept of an off state is often either misleading or irrelevant. Devices that appear “off” may actually still be sensing or processing data. And devices that appear “on” may be performing a vast array of operations.

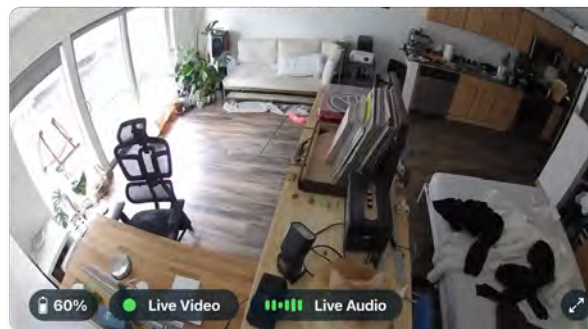
An LED indicator may seem like a small point. Yet it is the sole source of feedback for any user without app access. Because most smart devices lack screens, on-device indication is a critical interface for adjacent users. Unfortunately, it is severely neglected in smart product design. Current smart cameras typically rely upon a single, and highly ambiguous LED indicator. We find that both primary and adjacent users distrust these indicators.

To improve trust and transparency, Arca’s on-device indication system clearly defines a True On and True Off state. The in-app indication system parallels the iconography and clarity of the on-device indication.

The True On and Off indicators were designed to intuitively communicate states to adjacent users without requiring instruction.

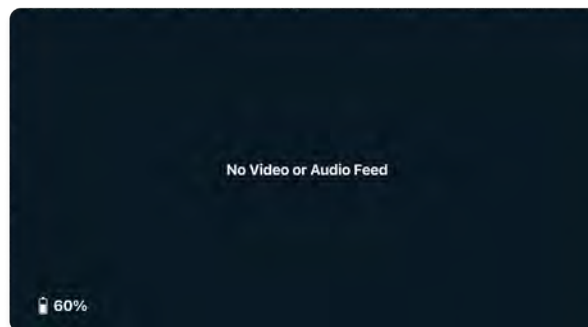
A more subtle function of True On and Off states is to anchor users’ mental model with a floor and ceiling for each sensor. Medium and Strong privacy conceptually fit “in between” the True On and Off states.

True On



True On indicates that the camera’s sensors are fully “open and active:” the device is recording and any number of event detection states may be active. On the device, True On is represented by a green ring and dot. The camera True On indicator is represented by a green ring that encircles the lens. The mic True On indicator is represented by a point light in proximity to the visible microphone grating. In the app interface, True On is indicated with parallel iconography. In competitor apps, it is difficult to discern if the microphone is enabled in the app view. To correct this, Arca displays an eye-catching animated sound bar icon to communicate that the microphone is active.

True Off



True Off indicates a sensor is completely deactivated and unable to record video, detect events, or perform any other functions. On the device, True Off is indicated with an unlit indicator. The camera True Off state is additionally indicated with an electromechanical cover that encloses the lens. In the app interface, True Off is indicated by dark field of view with text confirming the camera is truly off.

Medium Privacy

✖ A Reversible Privacy Default

Medium Privacy mode adds a removable mask that blurs video and muffles audio. Owners can always unmask video to review events, but other users may be notified. Further, unmasked video is watermarked and the time and user who unmasked the video is visible in the history view.

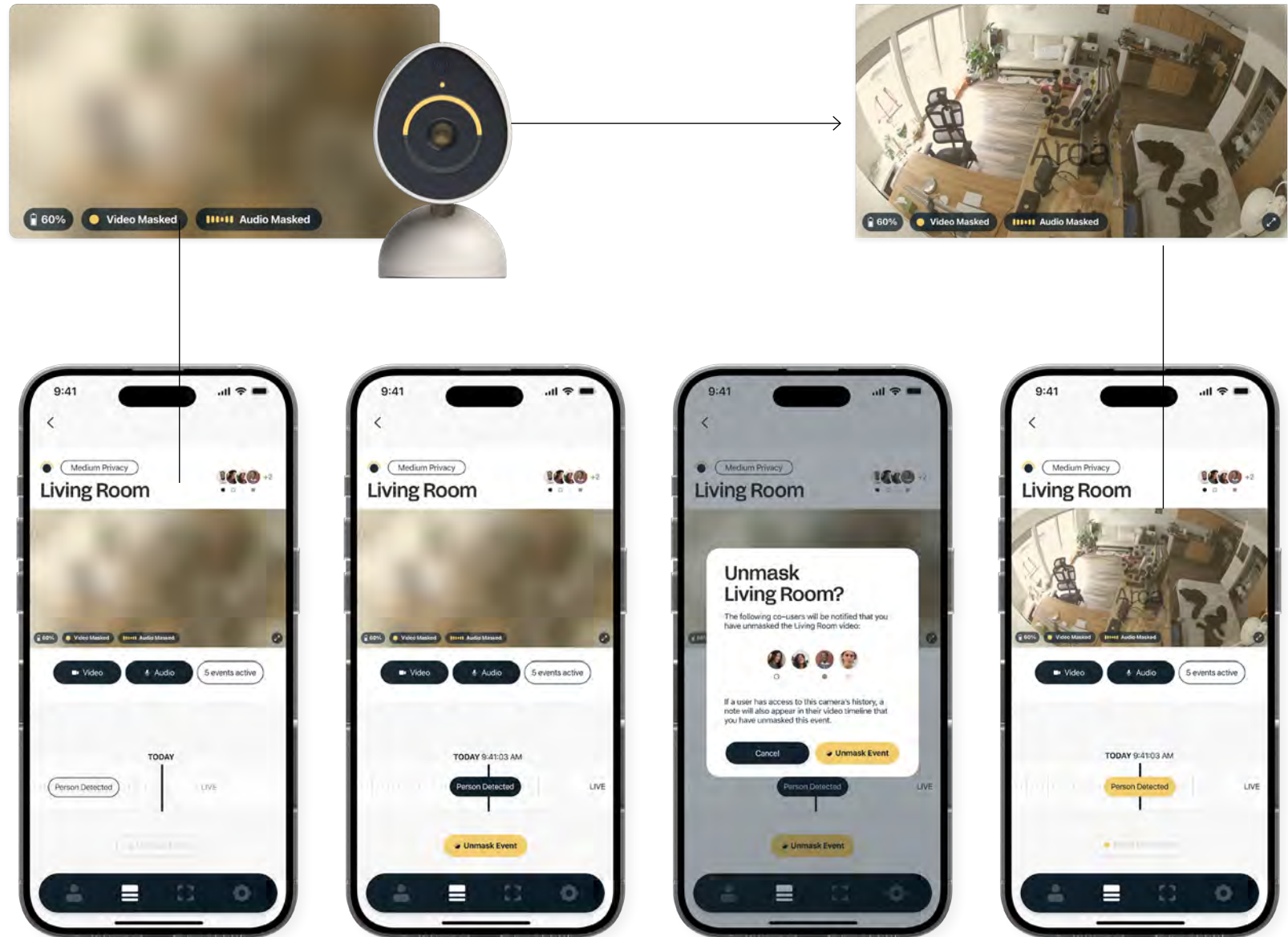
Medium Privacy is designed to discourage owners and other co-users from reviewing videos of their household, guests, neighbors, and so on. Unmasking video is a somewhat tedious process, and the unmasking feature holds users socially accountable by notifying other users if video is unmasked.

This gives primary users and their household a **double peace of mind**: Peeking is discouraged, but it's always an option if something happens.

✖ Example Use Cases

Informed by situations described by participants in our studies, the following are specific cases where Medium privacy may allow households to achieve a suitable compromise:

- A parent wants to monitor their home for safety issues or their teenager throwing a party while they're away. But they also want to respect their children and spouse's autonomy.
- Neighbors in a 4-unit apartment building want to setup a shared camera after a recent break-in, but don't want to be spied on—and may not fully trust each other.
- A sibling installs a smart camera to monitor their disabled family member and their caregiver who live far away. They want to assure everyone that they will not review any video unless an incident occurs.



Unmasking video to review an incident. Any user with Owner status can unmask any recorded video or audio. However, this is subtly discouraged in several ways.

Access Speed bumps. Unmasking video is deliberately tedious. Segments must be unmasked manually. The unmasking option is hidden several layers deep in the information architecture.

Social accountability to co-users. Co-users—such as family members, roommates, or nannies—will receive a notification when video is unmasked.

Watermark and history for transparency. A record of who unmasked a video and when is permanently logged. Unmasked video is watermarked, which may inhibit posting video online.

✖ Detect, But Don't Record

Strong Privacy mode fully disables the cam/mic from recording. But users can still be notified with text descriptions of events—like when the kids arrive home, or the cat is chewing on plants. Strong Privacy allows a household to monitor for important events while providing a high level of privacy preservation.

✖ Rules

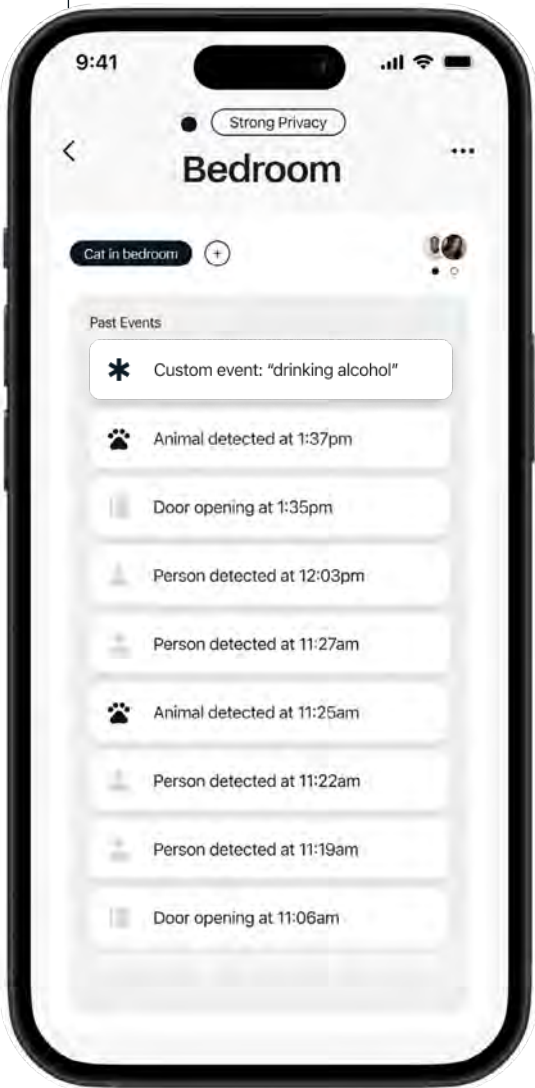
The real power of Strong Privacy lies in the ability to create custom Rules where events trigger automatic mode switching. For example, Exception Rules can be setup that automatically switch a camera from Strong Privacy to True On whenever smoke is detected or an unfamiliar face is seen.

Rules can also be creatively defined to allow mode switching with facial recognition or gestures. For example, a rule could be created to allow a pet sitter or family member to deactivate the camera by looking at it and waving.

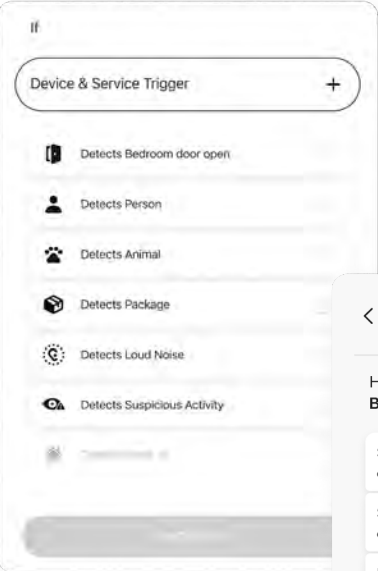
✖ Speculative Event Detection

Our design inquiry is not solely focused on adjacent user privacy but also explores emerging harms and benefits of smart devices. Arca also explores advanced, custom-trained events such as identification of smoking, yelling, profanity, screen use, nudity, license plates, and wild or exotic animals. As such events become more common, so too may the need for robust privacy modes and rules. While some of these capabilities are speculative, all UX features in this pictorial—interfaces, indicators, privacy modes, and rules—were built with interactive prototypes.

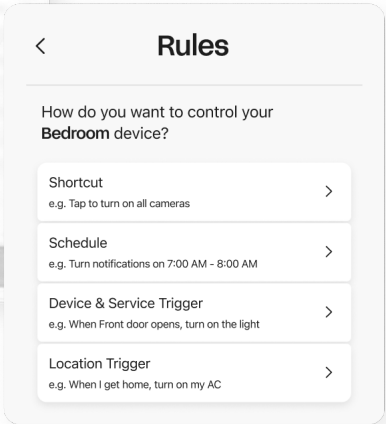
Event histories and notifications. A full history of events is also logged in the history view. Users can receive smart-phone notifications. The app allows rapid switching to True On to view live video.



Event descriptions and notifications. A brief description is presented whenever an event is detected. Recent events are display on the control panel view. Users can also receive event notifications.



Rules. Simple or complex Rules can be created for automated mode switching. A wide range of Events serve as the primary Trigger for Rules.



✖ Enabling Differential Access

Other smart cameras offer a one-size-fits-all approach to sharing. Arca allows users to customize who you do (or don't) share access with. The options range from equal Co-Owner to a limited Status View for letting neighbors, tenants, or workers know the location and privacy mode of devices.

With **Status View** owners can share only basic information about the settings or location of your device. For example, owners can use Status View to show a guest where their cameras are located and demonstrate that they are set to a privacy mode.

Status View is a versatile feature that allows users to customize the information they share with neighbors, guests, or tenants. For example, users can create a **Neighbor View** that demonstrates to a next door neighbor that the camera is not violating their privacy. Used in conjunction with our **Privacy Zone** feature, users can segment a portion of the field of view to block a neighbors' property. Status view allows the neighbor to verify it.

If an owners wants to inform others but without sharing access, they can instead send them Arca's **Shareable Mode Guide**. This allows adjacent users to learn about the different modes, and have greater trust that their privacy is being protected.

If owners want to give someone more access, Arca allows them to select from 3 tiered levels. **Co-Owner** grants full access. **Basic Controls** grant access to displays and mode selection, but does not allow more advanced settings like sharing access or configuring events. **View Only** limits access to live video/audio and recorded timeline events. If none of these are suitable, owners can create a **Custom** category of shared access.

ARCA

1h ago

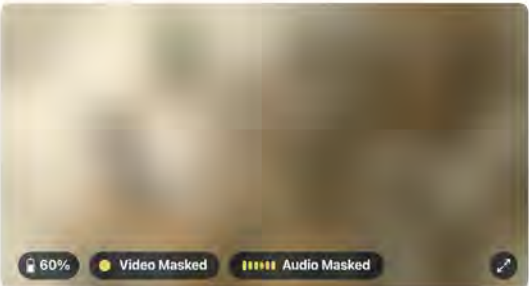
John switched the Kitchen camera from Normal to Medium Privacy.

Medium Privacy



Kitchen

View Only



60%

Video Masked

Audio Masked

Privacy Mode

Camera is set to "Medium Privacy" mode. In this mode, there is a removable privacy mask that blurs video and muffles audio.

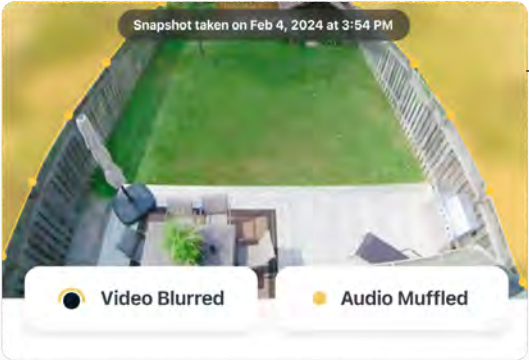
Camera Location



Note from the owner:
"The camera is on the shoe rack"

Camera Users

2 other users have access to this camera.



Camera Users

Steven

Owner

Aaliyah

Co-owner

Kiana

View Only

Nadine

Status View

Nate

Basic Controls

Reuben

Configuring and Sharing Privacy Zones. Owners can define zones within the camera field of view. Each zone can be placed in a separate mode, such as True Off or Medium Privacy.

A few current smart home cameras, such as Amazon's Ring doorbells, allow users to block their neighbor's property from view. However, neighbors have no way to verify. And owners have no mechanisms for demonstrating they are a good neighbor. Neighbor Status View solves this problem showing neighbors a preview of the masked area coupled with a promise that they'll be notified if the zone is modified.

Managing Share Access. To encourage sharing, owners are able to access a full list of users and their level of access from most key screens of the app. Adding, deleting, updating, and pausing access is simple.

Customizing Status View. Owners can customize status view to share device information including the current mode, and image and description of the camera's location, a preview of what the camera can see, active events and rules, and who else has access.

✕ Details

We wanted different audiences to engage with Arca as a realistic possibility. These audiences include design and research communities but also members of the public. We also wanted to truly determine if our abstract concepts could be successfully implemented as a fully functional interface. We thus devoted significant effort to design details often omitted in design research.

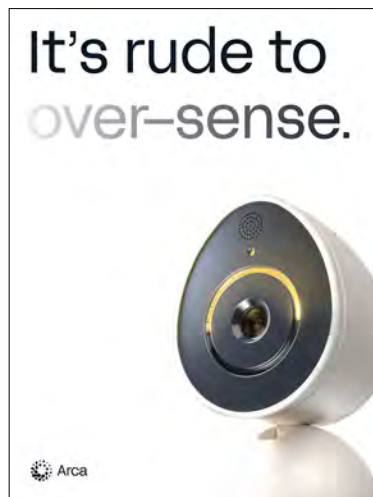
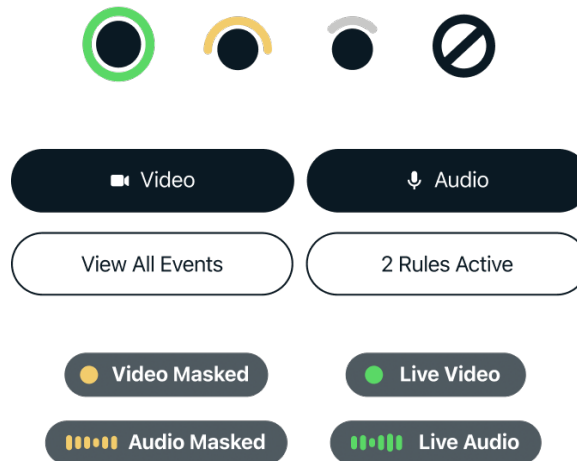
✕ Branding

Connection and being part of a greater whole is a key to the Arca brand. They concentric dots of the logo suggest interconnection. The combine to convey an image of an abstracted camera lens. We avoid obvious imagery of an eye and its negative associations with surveillance. The Arca name connotes arches and circles. This is a reference to Arca's inclusive indication system. It is also a metaphor for connecting primary and adjacent users.

✕ Speculative Marketing

Arca is not only a proposed solution. We designed Arca to also function as a provocation capable of engaging different audiences. What if companies prioritized the needs of adjacent users, instead of focusing on their more profitable primary users? Is Arca a good solution? Or, to the extent that it supports surveillance, is it actually part of the problem?

Internally, we thought of Arca as a subtly speculative design. To signal this intent, we created a second layer to our design in the form of a speculative marketing campaign. Our branding posters challenge primary users with slogans such as "Surveil responsibly" and "It's rude to over-sense."



✕ Design System

We developed a robust design system that included basic branding and interface components, such as type ramps, buttons, cards, indicators, motion, and microinteractions.

Later, we elaborate other aspects of our design system, including high-level design patterns and principles. On the following page, we outline our general approach of creating an Inclusive Indication System that coordinates in-app and on-device feedback to communicate with primary and adjacent users.

✕ Form Language

The form language of the camera conveys trust and stability, but counterbalanced with a sense of approachability. Visible microphone grating and tactile lens covers reflect Arca's commitment to transparency. Soft curves and choreographed indicator transitions add subtly playful moments to an otherwise serious product.



✕ Inclusive Indication Systems

Arca is designed to better support diverse and sometimes conflicting needs of many different users/subjects. While Arca still privileges a primary user, the interface is intended to actively encourage device owners to extend awareness, consent, access, control, or benefits to adjacent users.

Arca's specific indication system illustrates a much more general idea: designing more inclusive external indicators and internal states for smart devices. We refer to this as an Inclusive Indication Systems. Inclusive, in this context, does not imply that everyone's needs are met equally, or at all. Rather, it simply indicates that the system is designed with adjacent users in mind.

Here we show how the concept underlying Arca's Inclusive Indication System can be extended to other technologies and contexts.

✕ Speculative Infrastructures

Inclusive Indicators are just the experiential tip of the iceberg. Beneath the surface, they must be supported by computer hardware, code, and data. In some cases, they may even require new policies and laws. Think of the US WiFi medical device guidelines or the EU General Data Protection Regulation (GDPR).

To expand the possibilities for Inclusive Indication Systems, we use Arca to imagine new interface-infrastructure systems. For example, we speculatively envision a universal standard for a Beacon protocol that broadcasts inclusive indicators and states. We also imagine new laws requiring the implementation of Beacon Indicators in public devices, like smart cameras.

✕ Straightforward Extensions

Additional Privacy States: Extending the “open/closed” metaphor.

The open/closed metaphor can be extended to indicate more than two “in between” states. Though this approach has clear perceptual and conceptual limits.



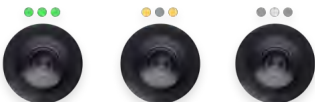
Bar Implementation

Arca's indication system is not limited to circles and arcs. A bar implementation, for example, can be used instead.



Point Light Implementation

Three RGB point lights can be used to implement Arca's indication system. This is useful for cost-sensitive applications, like public security cameras.



✕ A Universal Status Beacon Protocol and Icon

What if there was a standardized network protocol specifically designed for broadcasting IoT status information? Such a protocol would enable device owners to publicly share the “keys” for deciphering their on-device indication systems. Additional information could also be shared, such as the purpose of the device, or the name and ID of its owner. Owners might share this voluntarily, or to comply with new legal requirements.



✕ E-Ink Lens Covers

Electric ink creates many opportunities for more advanced functional and aesthetic applications of sensor overlay indicators. For example, aesthetically intriguing privacy masks applied to video can be represented with e-Ink lens covers.



✕ Emerging Applications

Looking forward, we can expect to see many new smart devices with spatial sensors. Some of these will surely surpass the smart camera in terms of pervasiveness and power to invade the privacy and freedom of others. Here we envision Inclusive Indication Systems applied to new and emerging applications with cameras and microphones. Other spatial sensors systems, such as GPS, Wifi, lidar, radar, and infrared cameras should also be considered.



Robots, such as Amazon's domestic robot Astro, would benefit from inclusive indication systems.



Mixed reality and spatial computing products, such as Apple's Vision Pro, might employ Arca-like indicators to communicate with adjacent users.



Wearables and generative AI applications, such as the Humane AI Pin, could increase trust with modes similar to Strong Privacy to protect users from “always on” microphone and camera sensing.



Conventional smart cameras are used in many contexts beyond the home, such as small businesses, caregiving, and public spaces. When combined with Beacons or Shareable Mode Guides, inclusive indicators can provide workers, clients, patrons, and citizens improved peace of mind.

✕ Generalizing Knowledge

Arca blurs boundaries between functional prototypes, speculative products and critical reflection. It serves as a platform to explore new possibilities and expose limits of user-centered design. From the outset, our goal was to generalize insights for other sensor-enabled devices. We present knowledge in the form of design patterns, principles, and problem framings—grounded in prototyping and user testing with primary and adjacent users. We approached Arca not simply as a solution, but as a mode for discovery through making. Through iterative making, situated testing, and reflection, we surfaced patterns and principles that would have been difficult to derive through theoretical speculation or conventional usability studies alone.

We argue that our knowledge products (design patterns, principles, and issues) have value independent of any empirical validation. Just as engineering researchers produce technical proof-of-concept and humanities scholars make conceptual constructs, **we believe that research through design can create exemplary artifacts**, such as Arca and the generalized design knowledge we present within this text.

Issue: Over-sensing, Under-reacting **Response: Clear but Nuanced States**

Smart sensing devices tend to over-sense and underreact. By default, sensors are designed to absorb as much data as possible. However, maximum sensitivity is often not needed or not worth the cost of privacy invasion. Like all computing technologies, smart devices suffer from the basic “black box” problem of opaque inner-workings. However, these issues are compounded with IoT devices which typically lack computer screens. Feedback is primar-

ily delivered through smartphone apps, which generally exclude impacted adjacent users. Arca illustrates several design patterns for addressing these issues.

True On and Off. “On” and “off” states make sense with simple devices like lamps. Digital devices with sensors, network communication, and data processing capabilities are an entirely different story. Arca exemplifies a True On/Off design pattern that can be applied to any smart sensing device.

In contrast to Medium and Strong Privacy, True On/Off states are designed to be easily inferred by adjacent users without additional instruction. This was validated across our user studies.

Principle: To improve transparency and trust, designers should clearly define two contrasting states for each sensor: A True On state that represents its most active and sensitive state, and a True Off state where the sensor is completely deactivated. True On and Off help anchor a user's mental model of operation. They represent the conceptual floor and ceiling of device's most and least sensitive, and invasive, states.

Sensor Dimmer Switches. Smart product designers need to create better controls and indicators that allow users to achieve and understand complex states “between on and off.” To enhance privacy, Arca employs a more general design pattern of a sensor dimmer switch. Arca offers two primary states between True On and Off: Medium and Strong Privacy. **Principle:** Offer Sensor Dimmer Switches for configuring privacy-enhancing states between true on and off.

Inclusive IoT Indication Systems. Design systems—an essential tool for interaction design—are comprehensive guidelines, standards, and reusable

components that ensure consistency and efficiency across a product's user interface and user experience. However, smart product designers focus most of their energy on apps to the neglect of the humble indicator light and sound.

By focusing on the overlooked needs of adjacent users, we surfaced the neglected importance of designing inclusive indication systems for IoT devices. Arca required us to develop a better vocabulary for indication systems, such as the interplay between in-app and on-device indicators. On-device indication typically uses space-constrained indicators such as LED lights and sound from digital speakers. HCI research has shown that more expressive light indicators are possible 22.

Perhaps the most novel inclusive indication pattern we introduce is the concept of a physical **sensor overlay indicator**. They serve to both functionally and symbolically enhance transparency and provide an extra layer of trust.

To allow custom indicator display without compromising trust, Arca's indicators can be minimized but not disabled. This illustrates a technique of **correspondence integrity** that achieves trust through reliable state mapping.

Arca's indication system was attentive to the accessibility needs of color blind and low vision users. We are currently finalizing Arca's audio indicator system, which prioritizes vision impaired users.

Issue: Horizontal Surveillance **Response: Discourage Access**

Whether its deliberate, accidental, or somewhere in between, primary users are surveilling adjacent users—including family, friends, neighbors, employees, and passersby 51. While we may not be able to prevent the most egregious and harmful forms of everyday surveillance [3, products can discour-

age casual or unnecessary invasions of privacy.

Access Speed Bumps. Arca illustrates how an interface can inhibit users from surveilling other users while still allowing them to do so if needed. In Medium Privacy, users can unmask video. However, unmasking is a somewhat tedious process that requires manually selecting segments of a recording and tapping multiple buttons to finally view the original video and audio.

Both primary and adjacent user participants saw value in this feature. They readily grasped the concept of a speed bump as a willfully self-imposed barrier. As one user remarked, “It makes me pause to say: Do I really wanna see this? That has good privacy implications.”

We refer to this design pattern as data access speed bumps. Like vehicular speed bumps, interface access speed bumps promote self-restraint for a greater good. **Principle:** Create access speed bumps to discourage use of features deemed necessary but with high potential for misuse.

Social Accountability. Arca illustrates three mechanisms for improving privacy through social accountability: notification, logging, and watermarking.

Unmasking video requires that users first confirm that shared users will be notified. This encourages them to act prudently. The history view displays a log of who unmasked which videos. Unmasked video is watermarked to show that the camera was a set to a private mode. This may discourage users from sharing or posting video to social media unless the situation truly demands it.

In general, social accountability techniques convey a social contract enacted with Medium Privacy modes, along with norms of acceptable behavior.

Issue: Power Imbalance **Response: Share the Interface**

Inadequate disclosure and poor communication is a source of interpersonal tension and conflict with everyday surveillance technologies. We found that adjacent users are often less concerned about the personally sensitive content of video. They are upset because they feel disrespected and disempowered.

Tokens and gestures. Extending partial access and control to adjacent users can make them feel empowered, respected, and informed—even if they don't actually use it. It can also open opportunities for primary users to disclose devices and customize access on a case-by-case basis.

For example, a nanny who participated in our user study explained that Arca's features might “change the conversation [with employers] so we can discuss and decide what's comfortable for all of us.” **Principle:** Include features that enable primary users to extend access. Even if they are not directly used, these features may prompt improved communication and respect between primary and adjacent users.

Device Status Sharing. Primary users understandably are reticent to give others access to their devices. By providing differential access, smart products can encourage primary users to better inform and solicit consent. Arca illustrates a specific differential access technique of Status Sharing. Adjacent users can be offered limited app access to explain and verify a device's status—such as basic operation, location, and users/owners—even when other permissions are not needed or desired. **Principle:** Provide Status Sharing features that enable primary users to inform others without giving them access to sensitive data or settings.

✕ Going Deep to Learn Broadly

Arca was the culmination of two intensive years of design research. Our process included stakeholder interviews, design audits, competitive analysis, novel problem-framing, exploring divergent design directions, focus and refinement, iterative testing, and the production of prototypes and other communicative materials. Here we chose to narrowly scope our presentation around our final design artifact and knowledge products.

While we initially scoped our research broadly and explored a wide range of design concepts, there was a turning point in our process where we became intensely focused on designing a viable solution. We pursued this similar to how a company would go about developing a real product. At times we wondered whether it was worth the level of work we were investing in details such as logos, branding, indicators, and robust visual design systems.

Ultimately this level of depth paid off in unexpected ways. For example, our

narrow focus on designing better indicator lights brought into focus a much broader opportunity to define and communicate complex states between on and off. Our close attention to indicator lights also led us to generalize design patterns such as True On and Off, and Sensor Dimmer Switches. This work surfaced a broader need to develop Inclusive Indicator Systems for IoT devices with more thoughtful and advanced on-device indication.

These and many other forms of knowledge emerged through a similar pattern: **Going deep enabled us to arrive at more general insights** [25].

✕ Anticipating Futures

From the outset, we recognized that Arca's most advanced features might have limited applications. They are most useful in specific contexts or situated actions, such as parents with nannies, neighbors in a shared apartment building, adults caring for their aging and disabled family, and owners of vacation rentals (all real examples from our primary user interviews).

However, we embarked on this design process with an eye toward the future. Our assumption was that the need for features like Strong Privacy, Flexible Sharing, and True Off will increase as sensors and surveillance continue to become a normal and accepted part of everyday life—for better, or for worse.

At times, we intentionally envisioned new functionality that would exacerbate privacy harms and power imbalances. For example, we designed powerful, and creepy, forms of event detection such as “aggressive behavior,” “smoking and drinking,” and “specific words or phrases spoken.” Guided by research on machine learning appli-

cations for computer vision and object recognition, we envisioned these features to anticipate future privacy needs and power imbalances.

Arca provided us a platform to speculative beyond the literal product. Previously we discussed how speculative design concepts might inform the creation of new laws, policies, and technical standards. For example, we imagined new laws requiring public businesses to use features such as Status Sharing or Medium Privacy on their smart cameras.

We also surface broader AI ethics issues—such as over-detection, creepiness, and surveillance normalization—highlighting a need for restraint and transparency in future infrastructures.

✕ Testing Limits

We set out to design Arca knowing that no optimal solution existed. Equally satisfying primary and adjacent users is an intractable problem. We knew we would need to make compromises that would benefit some at the expense of others. We also knew that adjacent users would remain at a disadvantaged position. We did not like this fact, but we also did not hide from this reality.

We engaged with this challenge partly to explore what smart product design interventions were possible, and which were not. With time, we embraced our challenge as a way of testing the very limits of human-centered design solutions and approaches.

Early on, we recognized that we would need to persuade primary users to extend power to adjacent users. Without fundamental changes to laws and norms, primary users would remain in control of their devices and property. To us, this suggests a limit point of inter-



active product design to enact change.

✕ Engaging Others

More generally, our research hit upon specific instances of fundamental limits to user-centered design philosophies. For example, consider Principle #1 of Jakob Neilson's famous usability heuristics: “Visibility of System Status - The design should always keep users informed about what is going on, through appropriate feedback within a reasonable amount of time.”

Our research demonstrates the limits of this principle and other single-user thinking. With smart cameras, primary and adjacent users often hold competing needs for visibility of system status. For example, a primary user may desire enough visibility to alert an intruder, but not so much that it attracts the attention of disapproving neighbors. A neighbor may wish to know the precise location and status of the camera—as does a potential thief or vandal. This problem is compounded by the constraints of on-device indicators, which must communicate to all users and with economical, space-constrained forms.

Arca translates abstract ideas into concrete forms. These forms are accessible to many audiences. We have used Arca to engage many different types of people including camera owners, domestic workers, designers, engineers, artists, and members of the public. We continue to disseminate this work through public exhibitions, demos, intellectual property, and design competition awards [24]. Transcending our particular concerns with privacy, power, and smart products, Arca illustrates the potency of design research artifacts to function across multiple registers to engage. This work emphasizes that adjacent users are not just passive bystanders, but key stakeholders whose needs and experiences must shape the future of smart device design.



✕ Acknowledgments

This research was supported in part by National Science Foundation Grants 1910218 and 2142795.

✕ Arca Project Team

Many have contributed to this project, including work that was not included within this Pictorial but has contributed to broader Arca project.

Principal Investigator, Design and Research Lead: James Pierce

Context + User Research: Robyn Anderson, Claire Weizenegger

Interaction + Visual Design: Lian Bensaadon, Faith Ong, Burke Smithers, Hope Terpilowski, Wyatt Olson

Industrial Design: Ann Lai, Cole Young

Physical Computing and Interactive Prototyping: Chongjiu Gao, Wayne Jiang, Sergio Medina, Franziska Roesner

Early-Stage Design: Isha Agarwal, Robyn Anderson, Parag Nandi, Claire Weizenegger, Gwenna Gram, Jade Hurle, Jackson Jiang, Betty Lo, Camille Miller, Aaron Park, Aivy Phan, Mark Schumskiy, Grace Sturlaugson

✕ References

- 1 Alexander, C. (1977). *A pattern language: towns, buildings, construction*. Oxford university press.
- 2 Ahmad, I., Farzan, R., Kapadia, A., & Lee, A. J. (2020). Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), 1–28.
- 3 Andrejevic, Mark. (2004). “The work of watching one another: Lateral surveillance, risk, and governance.” *Surveillance & Society* 2.4
- 4 Baumer, Eric P.S. (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.
- 5 Berger, Arne, 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.
- 6 Bernd, Julia, 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.
- 7 Brand, Nico, 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.
- 8 Brunton, Finn and Helen Nissenbaum. (2015). *Obfuscation: A user’s guide for privacy and protest*. MIT Press.
- 9 Chalhoub, George, 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.
- 10 Chen, Yuxi, 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.
- 11 Cheng, Yu-Ting, 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.
- 12 Cila, Nazli, 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.
- 13 Desjardins, Audrey 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.
- 14 DiSalvo, Carl, Tom Jenkins, and Thomas Lodato. (2016). Designing Speculative Civics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI ‘16)*. Association for Computing Machinery, New York, NY, USA, 4979–4990.
- 15 Dunne, Anthony, and Fiona Raby. (2013). *Speculative everything: design, fiction, and social dreaming*. MIT press.
- 16 Ehrenberg, Nils 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.
- 17 Fiesler, Casey, 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,
- 18 Freed, Diana, 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.
- 19 Frik, Alisa, 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).
- 20 Gaver, William. (2012). “What Should We Expect from Research through Design?” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 937–46. Austin Texas USA: ACM.
- 21 Harvey, Adam. “CV Dazzle: Camouflage from Face Detection.” Accessed May 2, 2020. <https://cvdazzle.com/>
- 22 Harrison, Chris, John Horstman, Gary Hsieh, and Scott Hudson. (2012). Unlocking the expressivity of point lights. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ‘12)*. Association for Computing Machinery, New York, NY, USA, 1683–1692.
- 23 Inbar, Ohad and Noam Tractinsky. “FEATURE The incidental user.” *interactions* 16.4 (2009): 56–59.

- 24 IXDA Design Awards. (April 2024). Finalist: Arca: An inclusive, privacy-enhancing smart home camera for you and your extended household. Retrieved April 21, 2025: <https://awards.ixda.org/projects/arca.html>
- 25 Jarvis, Nadine, 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 (NordCHI '12). Association for Computing Machinery, New York, NY, USA, 11–20.
- 26 Jenkins, Tom. (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.
- 27 Jensen, Carlos 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.
- 28 Knowles, Brian, 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.
- 29 Kozubaev, Sandjar, 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.
- 30 Lau, Josephine, 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.
- 31 Lindley, Joseph, Haider Ali Akmal, and Paul Coulton. (2020). “Design research and object-oriented ontology.” *Open Philosophy* 3.1: 11–41.
- 32 Mare, Shirang, 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: 436–458.
- 33 Martin, Kirsten. (2016). “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.
- 34 Marx, Gary T. (2003). “A Tack in the Shoe: Neutralizing and Resisting.” *Journal of social issues* 59.2 (2003): 369–390.
- 35 McDonald, Aleecia M. and Lorrie Faith Cranor. (2008). “The cost of reading privacy policies.” *Isjlp* 4 (2008): 543.
- 36 McReynolds, Emily, 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.
- 37 Palen, L., & Dourish, P. (2003). Unpacking “privacy” for a networked world. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 129–136).
- 38 Pierce, James. (2014). On the presentation and production of design research artifacts in HCI. In Proceedings of the 2014 conference on Designing interactive systems (pp. 735–744).
- 39 Pierce, James. (2019). “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.
- 40 Pierce, James. (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.
- 41 Pierce, James, 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.
- 42 Pierce, James, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwen-na Gram, Jade Hurtle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. (2022). Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In Designing Interactive Systems Conference (DIS '22). Association for Computing Machinery, New York, NY, USA, 26–40.
- 43 Punctoojit, L., & Hongwarittorn, N. (2017). Usability studies on mobile user interface design patterns: a systematic literature review. *Advances in Human- Computer Interaction*, 2017(1), 6787504.
- 44 Rogers, Jon, Loraine Clarke, Martin Skelly, Nick Taylor, Pete Thomas, Michelle Thorne, Solana Larsen, Katarzyna Odrozek, Julia Kloiber, Peter Bihr, Anab Jain, Jon Arden, and Max von Grafenstein. (2019). Our Friends Electric: Reflections on Advocacy and Design Research for the Voice Enabled Internet. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 114, 1–13.
- 45 Stappers, Pieter Jan, and Elisa Giaccardi. (2017). “Research through Design.” In *The Encyclopedia of Human-Computer Interaction*, 1–94. The Interaction Design Foundation, 2017. <https://research.tudelft.nl/en/publications/research-through-design-2>.
- 46 Spaa, Anne, Abigail Durrant, Chris Elsdén, and John Vines. (2019). Understanding the Boundaries between making 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.
- 47 Tan, Neilly H., Richmond Y. Wong, Audrey Desjardins, Sean A. Munson, and James Pierce. (2022). Monitoring Pets, Deterring Intruders, and Casually Spying on Neighbors: Everyday Uses of Smart Home Cameras. In CHI Conference on Human Factors in Computing Systems (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 617, 1–25.
- 48 Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79, 119.
- 49 Truong, Khai N., Shwetak N. Patel, Jay W. Summet, and Gregory D. Abowd. (2005). “Preventing camera recording by designing a capture-resistant environment.” In *International conference on ubiquitous computing*, pp. 73–86. Springer, Berlin, Heidelberg, 2005.
- 50 Wong, R. Y., Valdez, J. C., Alexander, A., Chiang, A., Quesada, O., & Pierce, J. (2023). Broadening privacy and surveillance: Eliciting interconnected values with a scenarios workbook on smart home cameras. In Proceedings of the 2023 ACM Designing Interactive Systems Conference (pp. 1093–1113).
- 51 Yao, Yaxing, 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.
- 52 Zeng, Eric, Shirang Mare, and Franziska Roesner. (2017). “End user security and privacy concerns with smart homes.” Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). 2017.
- 53 Zheng, Serena, Noah Aporhorpe, Marshini Chetty, and Nick Feather. (2018). User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (November 2018).