Reflecting on the Multi-Functional Artifacts of Arca:
A Privacy-Enhancing Smart Device for You and Your Extended Household

Project Team
Principal Investigator, Design + Research Lead
James Pierce, University of Washington, USA

Interaction + Visual Design
Lian Bensaadon, University of Washington, USA
Faith Ong, University of Washington, USA
Burke Smithers, University of Washington, USA
Hope Terpilowski, University of Washington, USA

Industrial Design
Ann Lai, University of Washington, USA
Cole Young, University of Washington, USA

Physical Prototyping
Chongjiu Gao, University of Washington, USA
Wayne Jiang, University of Washington, USA
Sergio Medina, University of Washington, USA

Research
Robyn Anderson, University of Washington, USA
Claire Weizenegger, University of Washington, USA

Current smart home devices understandably prioritize the needs of a primary user/owner, who is typically the purchaser of the device and corresponding subscription plan. Yet smart home devices with cameras, microphones, location tracking, and other spatial sensing capabilities invariably impact the privacy of people nearby such as family, friends, guests, neighbors, and domestic workers. These individuals, whom we refer to as *adjacent users* (or adjacent subjects), often interact with smart devices indirectly and with minimal awareness, consent, control, or benefits. While research on bystander [2][25], non-primary user [11][24], and adjacent user privacy [19] [32] has emerged in response to these issues, there is little design research that has responded with either concrete design proposals or prototypes, or generalized design patterns, principles, and problems. We present a research through design project that highlights an overlooked need to design for adjacent users. We summarize several innovative features our work and conclude by generalizing design insights applicable to other contexts involving sensors, multi-user interaction, and privacy.

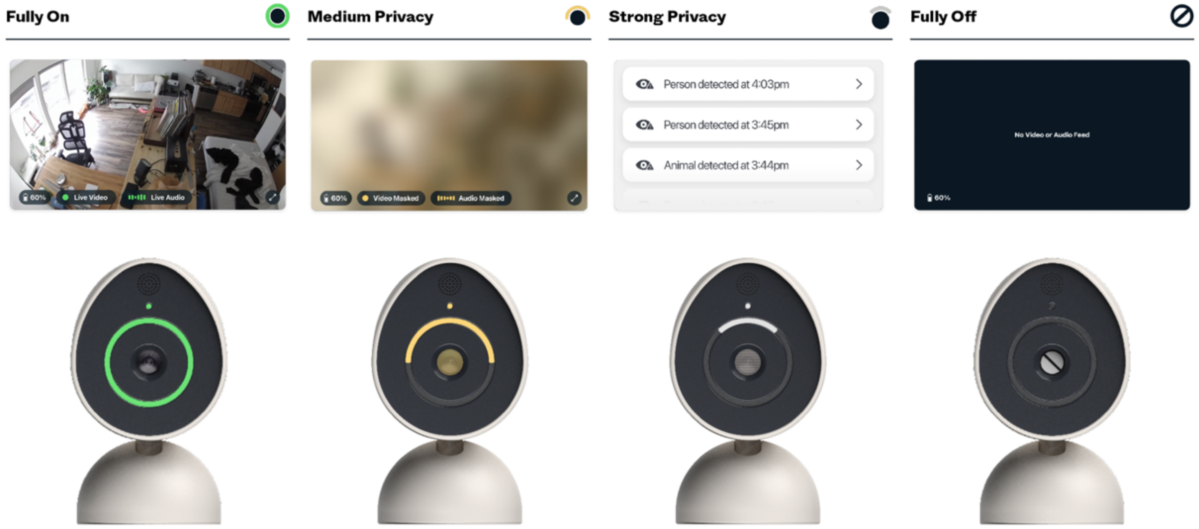


Figure 1: A novel on-device indication system: True On, True Off, and two "in-between" privacy states

1 INTRODUCTION

Digital privacy discourse tends to focus on relationships between individuals (users, customers, subjects) and powerful, surveillant organizations such as companies, third-party advertisers, governments, and cyberstalkers [9] and cybercriminals. This has been referred to as the vertical dimension of privacy [28]. 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) or (2) in a position of extreme, unassailable authority (e.g., the corporate online service provider or a government agency with a subpoena). The emerging discourse around "bystander privacy" foregrounds an orthogonal dimension we refer to more generally as horizontal privacy. This involves interpersonal, and often face-to-face relations between 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. When a horizontal relation is especially skewed, we sometimes refer to it as a diagonal relation. Diagonal relations are not as distant, abstractive, and authoritative as a vertical relation between user and a corporation, government, or cybercriminal, yet shares some elements of this power imbalance and impersonal social relation.

Our research finds that smart sensing devices pose significant privacy harms along the horizontal dimension, particularly between primary users who own and operate devices and adjacent users who have little or no direct awareness, consent, control, or benefit of smart devices that nonetheless may affect, and harm them. Our research with diverse users has uncovered recurring horizontal issues including interpersonal conflicts, reputation harms, and harms to personal autonomy and power.

Based on our extensive interviews with over 50 primary and adjacent users of smart cameras and related technologies (and supplemented by a review of related literature [e.g., [3][16][17][21][24][25][26]) we identify several core issues motivating our design: (1) Everyday surveillance. Primary users surveil adjacent users including family, guests, neighbors, and domestic workers. This surveillance may be planned and targeted, but often it is accidental or incidental. (2) Inadequate disclosure. Primary users rarely fully disclose smart devices or their surveillant capabilities and uses. Instead, disclosure is indirect, incomplete, and emergent. Many primary users considered or desired to disclose cameras but explained that they lacked mechanisms to do so safe securely and in a socially acceptable manner. (3) Interpersonal tensions. The nannies, pet sitters, houseguests, and neighbors we spoke to relayed experiences where inadequately disclosed smart cameras and poor communication led to personal discomfort and interpersonal tensions. Participants suggested that these privacy violations caused or accentuated feelings of distrust, resentment, indignation, and powerlessness. (4) Associative disclosure. Adjacent users such as nannies who also own and operate smart cameras reported higher trust and lower social tension with employers because they were familiar with the surveillance capabilities and uses. (5) 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). (6) Vertical trust/apathy. Most primary users describe high degrees of vertical trust, or else say "I can't do anything, so I try not to think about it."

2 ON, OFF, AND A FEW STATES IN BETWEEN

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.

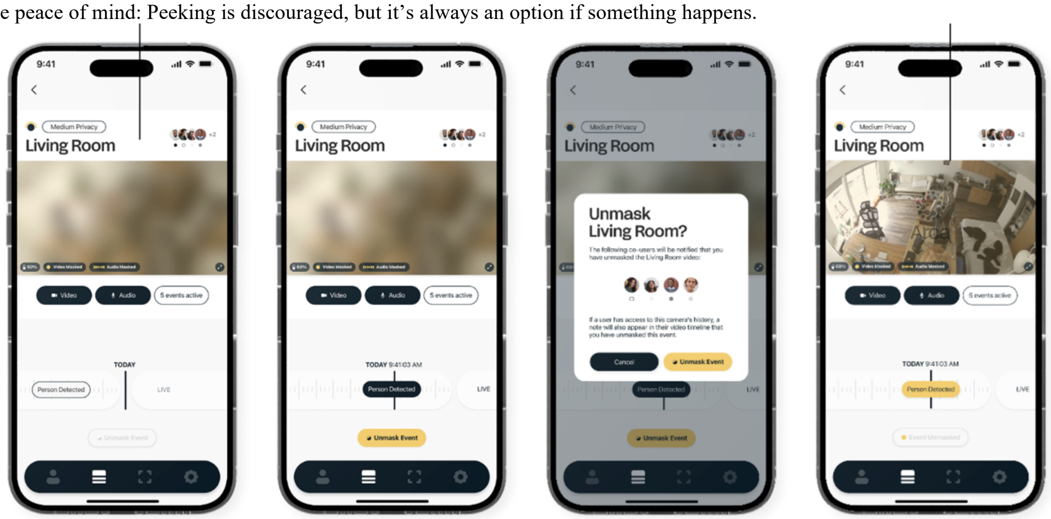
Improving on-device state indication. An LED indicator may seem like a small point. Yet it is the main form of feedback for any user who does not have app access, or cannot be bothered to open the app. Because most smart devices lack screens, we find that on-device indication is a critical interface that demands further research. One issue we identify with current smart cameras is that "on" and "off" are ambiguous states. A lit indicator can mean the camera is recording, the mic is recording, someone is live viewing or listening, the device is continually recording, the device is only recording short clips of events. Similarly, an unlit indicator can mean the device is idle but scanning for events, the battery is dead or software must be updated, or the user has disabled or blocked the indicator light but it is still recording.

True On/Off. To address these issues, we introduce a design pattern called True On/Off. True On indicates a sensor is active and recording to the app's history. True Off indicates a sensor is fully deactivated and unable to sense or record data. We further introduce separate indicators to disambiguate camera and mic sensors.

States "between" on and off. A second issue we identify is that primary users cannot easily control sensor sensitivity or data display to improve privacy for themselves and adjacent users. We introduce two novel privacy modes: Partial Privacy and Strong Privacy, which we discuss in detail later. A fuller indicator represents a more powerful (and more privacy-invasive) state. A diminished indicator represents a less powerful (and less privacy-invasive) state. The camera indicator is an LED ring the encircles that camera lens. It changes from a full circle to small arc depending. The mic indicator is an LED bar that borders the microphone. It ranges from a long bar to a small sliver.

3 MEDIUM PRIVACY MODE

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.



Unmask Living Room?

The following co-users will be notified that you have unmasked the Living Room video:

If a user has access to this camera's history, a note will also appear in their video timeline that you have unmasked this event.

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.

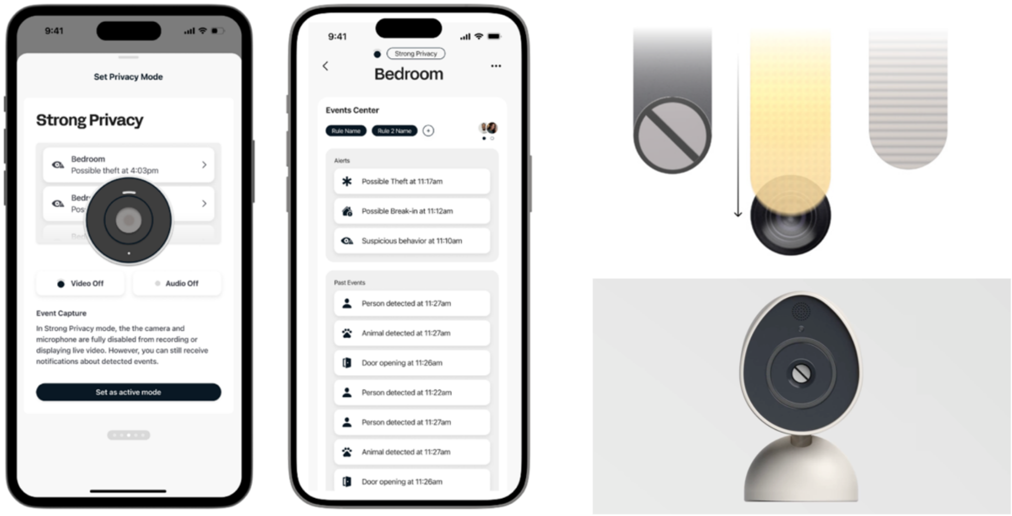
Figure 2: Medium Privacy Mode

4 STRONG PRIVACY MODE

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 speculative design inquiry is not exclusively aimed at solving adjacent privacy problems. We are equally concerned with understanding emerging harms and benefits of smart devices. In future work, we are designing more advanced and custom trained intelligent Events such as smoking, yelling, profanity, screen usage, nudity, license plates, police and fire, and wild and exotic animals. As more powerful events become more commonplace, the need for privacy modes and rules may increase.



Bedroom
Possible theft at 4:03pm

Event Capture

In Strong Privacy mode, the the camera and microphone are fully disabled from recording or displaying live video. However, you can still receive notifications about detected events.

Possible Theft at 11:17am

Possible Break-in at 11:12am

Suspicious behavior at 11:10am

Person detected at 11:27am

Animal detected at 11:27am

Door opening at 11:26am

Person detected at 11:22am

Person detected at 11:27am

Animal detected at 11:27am

Door opening at 11:26am

Figure 3: Strong Privacy mode (left) and Overlay Indicators (right)

5 FLEXIBLE SHARING

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 connection 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.

6 TEMPORAL DEPLOYMENTS

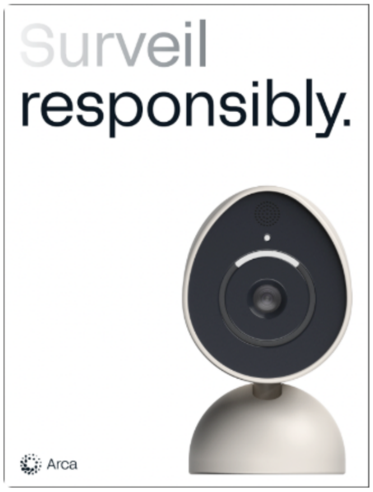
Over the past 2.5 years, this ongoing project has resulted in a **network** of artifacts and deployments that include:

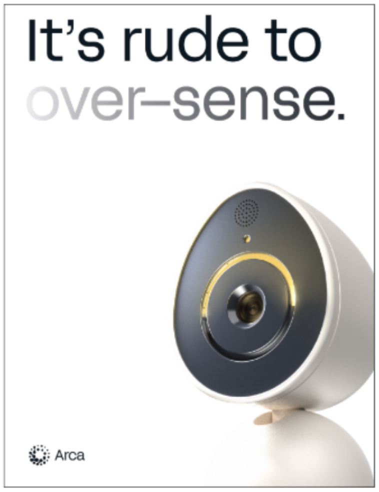
- Public exhibitions
- Design competition awards
- Provisional patent applications
- Concept videos
- Fictional branding campaigns
- Physical models and interactive computational prototypes
- Process and product documentation booklets for public and expert audiences
- Presentations and invited talks
- Multiple peer-reviewed publications
- Hands-on learning experiences for students
- Lab studies and concept evaluations
- Ongoing video production and broader dissemination activities

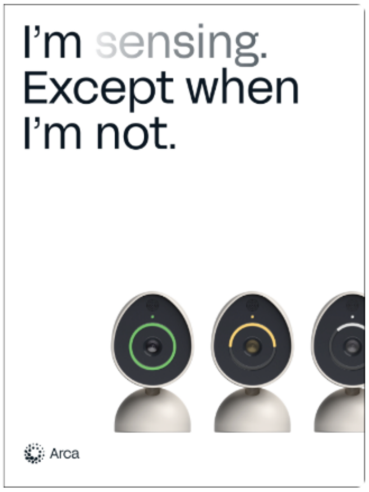
Arca is not a singular deployment study but rather an ongoing, emergent series of products and processes that we continue to use to generate new knowledge including (1) design patterns and principles, (2) exemplary design artifacts, (3) articulating limitations of user-centered design, and (4) exploring unconventional modes of disseminating research artifacts, including public engagement through concept videos, booklets, and exhibitions.

We've also reflected on how "going deep" into design details such as branding and design systems allowed us to arrive at more general insights, such as the design patterns and principles we've articulated across our dissemination materials.

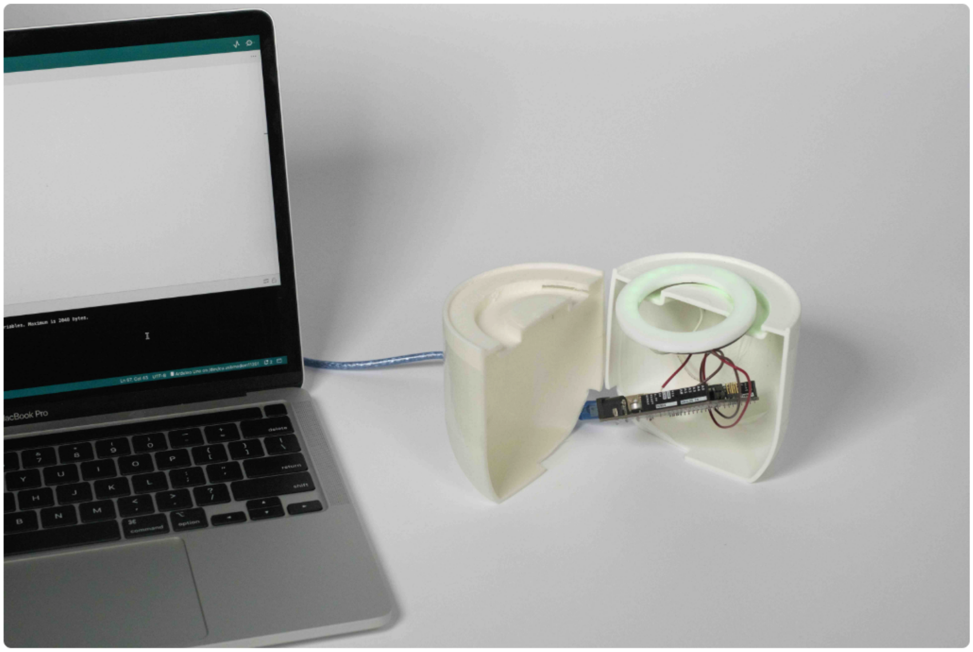
Appendix A: Selected Dissemination/Deployment Images

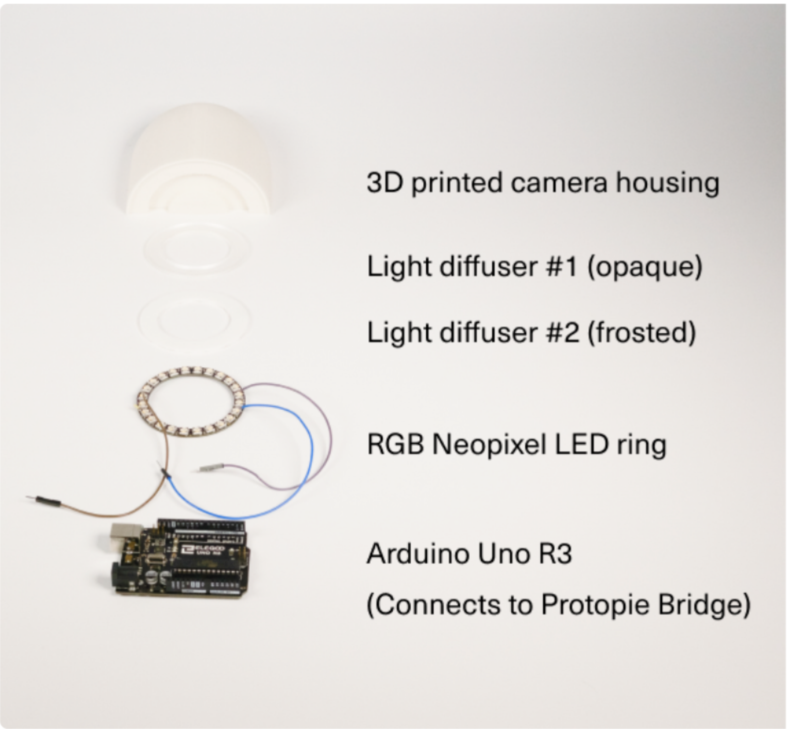


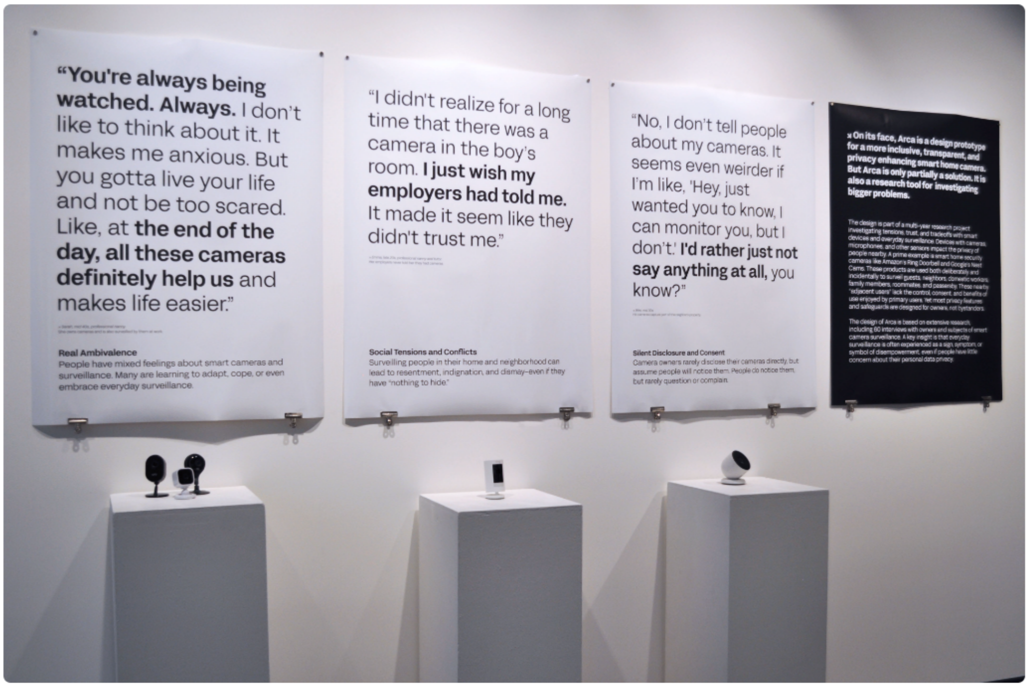




de to
sense.
On, Off, + a few
options in-between
Arca
If you just want guests to know the location or status of a camera, you can share only basic information without access to video or controls.
Living Room
Camera Us




3D printed camera housing
Light diffuser #1 (opaque)
Light diffuser #2 (frosted)
RGB Neopixel LED ring
Arduino Uno R3
(Connects to Protopie Bridge)



“You're always being watched. Always. I don't like to think about it. It makes me anxious. But you gotta live your life and not be too scared. Like, at the end of the day, all these cameras definitely help us and makes life easier.”

Real Ambivalence
People have mixed feelings about smart cameras and surveillance. Many are learning to adapt, cope, or even embrace everyday surveillance.

“I didn't realize for a long time that there was a camera in the boy's room. I just wish my employers had told me. It made it seem like they didn't trust me.”

Social Tensions and Conflicts
Surveilling people in their home and neighborhood can lead to resentment, indignation, and dismay—even if they have “nothing to hide.”

“No, I don't tell people about my cameras. It seems even weirder if I'm like, 'Hey, just wanted you to know, I can monitor you, but I don't.' I'd rather just not say anything at all, you know?”

Silent Disclosure and Consent
Camera owners rarely disclose their cameras directly, but assume people will notice them. People do notice them, but rarely question or complain.

On its face, Arca is a design prototype for a more inclusive, transparent, and privacy enhancing smart home camera. But Arca is only partially a solution. It is also a research tool for investigating bigger problems.

The design is part of a multi-year research project investigating tensions, trust, and tradeoffs with smart devices and everyday surveillance. Devices with cameras, microphones, and other sensors impact the privacy of people nearby. A prime example is smart home security cameras like Amazon's Ring Doorbell and Google's Nest Cams. These products are used both deliberately and incidentally to surveil guests, neighbors, domestic workers, family members, roommates, and passersby. These nearby "adjacent users" lack the control, consent, and benefits of use enjoyed by primary users. Yet most privacy features and safeguards are designed for owners, not bystanders.

The design of Arca is based on extensive research, including 60 interviews with owners and subjects of smart camera surveillance. A key insight is that everyday surveillance is often experienced as a sign, symptom, or symbol of disempowerment, even if people have little concern about their personal data privacy.

Appendix B

7 USER STUDY

Goals and Methods. Currently we are continuing to assess our prototypes with primary and adjacent user participants. To date we have conducted 6 semi-structured interviews with experientially diverse smart home camera users located in [major US cities]. Prior to this, we conducted a concept validation study of the initial design concepts for Shared Access and True On/Off with 11 participants. We also have conducted approximately 10 informal, iterative user tests with acquaintances at various stages of our design process.

The three main goals of our user study, in loose order of priority, are: (1) concept evaluation: assess whether and why our design features may or may not be useful, applicable, or otherwise valuable to primary and adjacent users, (2) exploratory study: more generally understand participants' preferences, experiences, and concerns with privacy, trust, control, inclusion, and social relationships with regards to smart devices, (3) preliminary usability testing: assess whether our specific design features are intuitive, learnable, accessible, and easy to use.

Our participant sample includes a diverse range of primary and adjacent users who have interacted with both indoor and outdoor cameras, including landlords, tenants, nannies, pet sitters, Airbnb guests, tutors, apartment dwellers with roommates, and families. This study was approved by our university's Institutional Review Board (IRB), and participants gave formal consent to participating in our study before engaging in the interview. The interviews took place via Zoom. They last about 60 minutes each, and participants were compensated with $50 in the form of Tango gift cards. Following an introductory discussion, we showed participants the interface design and interactions of the privacy features (see supplementary documentation). The conversation was facilitated using a semi-structured discussion guide (see supplemental documentation). In this pictorial we outline some preliminary findings from our user study. For brevity, we organize our findings into two categories: positive and negative findings.

Positive Validation. All participants grasped the basic use and functionality of Arca's main control panel, including the multiple camera feeds, separate video and audio controls, and display of shared users and active events. This granular level of visibility and control was exciting and empowering to many participants, prompting favorable comparisons to other less customizable smart camera applications. For example, one participant highlighted the value of the in-app and on-device audio indicators we introduced: "I find it helpful to have more control over whether you want to hear the audio or not, because in my case I almost never wanna hear the audio" (P4).

Across all participants, our design intent of the LED indicators was extremely well validated. Participants found True Off to be very intuitive, even without any instruction. Participants were also able to correctly guess and immediately understand which LED indicator referred to the mic, which referred to the camera, and which states indicated True On. As we expected, participants could not intuit the meaning of Partial and Strong Privacy indicators based on indicators alone. But as we hoped, once we introduced the features the indicators were easily learned and regarded as intuitive.

Many participants said that Arca's interface design prompted them to consider the privacy needs of adjacent users when they might not have otherwise done so. The Shared Access and Partial Privacy features in particular inspired participants to anticipate scenarios wherein they would willingly forfeit a degree of visibility or control to benefit adjacent users. Some participants articulated scenarios that incorporated the needs of domestic workers, while others only felt comfortable with scenarios that included closer relationships such as a spouse, friend, or roommate. Participants with personal experience as both a primary owner/user and as adjacent user were better able to grapple with the nuanced tradeoffs inherent in these features. They were more likely to consider and incorporate the privacy needs of adjacent users.

Of Arca's features, Partial Privacy and Unmasking were the most intriguing to participants. Most participants had never before encountered or considered this type of functionality. Some participants speculated that Arca's privacy settings might encourage them to extend their camera usage to areas of the home typically considered too private for surveillance, like the living room. "I could see [partial privacy] being intriguing, or like enticing to get people more comfortable, having cameras in their homes like how I was saying, like, we're not comfortable having a camera in the living room [currently]" (P5). Privacy modes and unmasking offered the most feeding ground for discussion.

One participant loved unmasking because it discourages surveillance with an extra step, which offers positive evidence supporting our "speed bump" design pattern for inhibiting viewing. Another participants expressed that the transparent viewing histories of Partial Privacy could facilitate better consideration and communication between users. "It makes them pause to say: Do you really wanna see this? And I think that has good privacy implications" (P4). Several participants expressed that our features hold potential to empower and encourage primary users to disclose devices and initiate better communication with adjacent users. One participant who had worked as a nanny recalled an instance when she discovered that her employer had been surveilling her without her knowledge for months. Her employers did not go out of their way to hide the camera, but neither did they directly notify her of its presence. She hesitated to broach the topic with her employers in part because she assumed a compromise would be impossible given the always on/off nature of smart cameras. Our design prompted this participant to imagine a scenario that enabled her and her employers to engage in an open dialogue about their privacy and security needs. "I think it would start changing the conversation…we can discuss and come up with what's comfortable for all of us." (P6)

Shortcoming, issues, and opportunities. As we expected, our study also surfaced many issues and limitations of our design. Some primary users/owners are still reluctant to consider the needs of adjacent users, unless there exists an established relationship (friend, family, etc). Many participants could not imagine scenarios where Partial Privacy and Strong Privacy would be helpful as a primary user: "Why would I want to see a blurry version versus just a full on version?" (P1). Not surprisingly, our study underscores that for many users and use contexts, people are simply unwilling to compromise and give up functionality for the benefit of others' privacy.

Overall unmasking sparked significant interest and all participants identified at least one use case where they could imagine using it. One participant for instance, identified value in the "Double accountability of unmasking that prompts conversations between users" (P4). However, we also found evidence that the unmasking feature could lead to a false sense of privacy and security. One participant stated that this feature only truthfully works if all actors are informed about the capabilities. Else, they thought it was deceptive. "If you were saying to people like, 'Oh, you're not being recorded right now' ... and then, later on, you could uncover that and actually see what was said or what was happening ... that makes me a little uncomfortable .... unless everybody knew that that could be a possibility ... its a little deceptive" (P5). One the one hand, this confirms our intent that Partial Privacy has limited utility unless you are utilizing Shared Access. On the other hand, this finding highlights that features like Partial Privacy has notable limitations for protecting the privacy of users excluded from Shared Access.

Some participants wondered where recordings "lived" and desired more information about storage, access, and duration of recordings. "Where's this stored? Is it being deleted, or is it permanently being stored somewhere? (P3)." This and related responses encourages us to continue developing other features we have begun to explore, such as better "data switching" controls for managing storage and duration of content.

Finally, we found that Strong Privacy seemed to hold the least value and presented the most uncertainty. As one participated explained, "I'm going to want to see what happened!" (P1). This suggests extreme reluctance to give up the ability to watch an event, particularly when the device is sending you an abstract notification that something has just happened. We continue to suspect that Strong Privacy can be highly applicable to contexts such as Airbnbs, workplaces, and domestic settings when properly configured with Rules and Exceptions. However, we have not yet tested Rules and Exceptions with participants to gauge if these indeed improve the usefulness of this feature.

8 DISCUSSION

Our design case study of smart home cameras is not simply about designing better smart cameras. Our research is structured from the outset to synthesize, test, and articulate broader design patterns and principles that may be applicable to other technologies, use contexts, and application domains. For example, some of our designs may have applications in workplace or industrial contexts. In the future, our design patterns and insights may have applications to domestic robots, drones, and wearables like smart glasses which are equipped with cameras and microphones. We conclude with a selection of design insights resulting from our research.

8.1.1 Sensor Dimmer switches: Data Attenuation Controls

In an age of digital, networked, and "always on" technology, the concept of digital "on" and "off" states can be virtually meaningless. We argue that smart product designers need to create better controls and indicators for complex states "between" traditional "on" and "off." To enhance privacy, Arca employs a more general design pattern we call attenuation controls. Partial and Strong Privacy modes allow users to attenuate, or diminish, the sensitivity of sensors or the display of data. The underlying metaphor is inspired by a dimmer light switch for sensors. Arca offers 2 primary states between True On and True Off: Partial and Strong Privacy.

8.1.2 Conceptual metaphors for complex states.

Indicating complex attenuation states between true on/off is a challenging endeavor. Our approach is twofold. First, we simplify to two intermediate states: a removable "partial privacy" mask mode, and an irreversible "events only with no video/audio recording" mode. Users can the customize many variations of these states with Rules, Exceptions, Events, and Shared Access. Second, we communicate theses states externally to all users through the on-device LED indicators. While a random person may not understand Partial or Strong Privacy, our evaluation suggests that an informed domestic worker, guest, or neighbor can. Further, our True On/Off states do appear intuitive to an uniformed passerby.

8.1.3 Speed Bumps and Social Accountability.

In most domestic contexts, smart home cameras are consumer products that are largely under the control of primary users. While laws, policies, and norms [8][23][27] guide their behavior, and design and engineering implementations dictate parameters of use, primary user ultimately have both the power and responsibility to consider the needs and experiences of adjacent users. Our features such as Partial Privacy and Shared Access are not designed merely as neutral options; they aim to invite, encourage, nudge, and persuade primary users to, in a sense, voluntarily limit and inhibit their surveillant users of their smart cameras. We employ 3 basic design patterns to achieve this. Partial privacy and unmasking employs a speed bump pattern to discourage, but not outright prevent the unmasking interactions by increasing physical and cognitive efforts. Partial Privacy and the unmasking option further employs a social accountability pattern by notifying users if video is unmasked and watermarking the video. Partial Privacy furthers additional involves a more subtle latent privacy safeguard pattern [21]: by discouraging users from unmasking, video and audio data is more likely to get auto-deleted thus preventing users from accumulating large repositories of saved video clips (many subscription services delete video after 30 days, and require tediously manually downloaded individual clips).

9 ACKNOWLEDGMENTS

[withheld for review]

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.

[2] 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.

[3] 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

[4] 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

[5] 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

[6] 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 . https://doi.org/10.1145/3357236.3395586

[7] 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

[8] 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

[9] 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

[10] 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).

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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] 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.

[18] 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.

[19] James Pierce, Claire Weizenegger, Parag Nandi, Isha Agarwal, Gwenna Gram, Jade Hurrle, Hannah Liao, Betty Lo, Aaron Park, Aivy Phan, Mark Shumskiy, and Grace Sturlaugson. 2022. Addressing Adjacent Actor Privacy: Designing for Bystanders, Co-Users, and Surveilled Subjects of Smart Home Cameras. In Designing Interactive Systems Conference (DIS '22). Association for Computing Machinery, New York, NY, USA, 26–40. https://doi.org/10.1145/3532106.3535195

[20] Anne Spaa, Abigail Durrant, Chris Elsden, 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.

[21] 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

[22] 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.

[23] 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

[24] 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

[25] 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.

[26] 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.

[27] Carl DiSalvo, 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

[28] Andrejevic, Mark. "The work of watching one another: Lateral surveillance, risk, and governance." Surveillance & Society 2.4 (2004