Smart Home Security Cameras and Shifting Lines of Creepiness

A Design-Led Inquiry

James Pierce

Design Division, California College of the Arts
San Francisco, California, USA
jpierce@cca.edu

CITRIS, University of California Berkeley
Berkeley, California, USA
pierjam@berkeley.edu

ABSTRACT

Through a design-led inquiry focused on smart home security cameras, this research develops three key concepts for research and design pertaining to new and emerging digital consumer technologies. *Digital leakage* names the propensity for digital information to be shared, stolen, and misused in ways unbeknownst or even harmful to those to whom the data pertains or belongs. *Hole-and-corner applications* are those functions connected to users' data, devices, and interactions yet concealed from or downplayed to them, often because they are non-beneficial or harmful to them. *Foot-in-the-door devices* are product and services with functional offerings and affordances that work to normalize and integrate a technology, thus laying groundwork for future adoption of features that might have earlier been rejected as unacceptable or unnecessary. Developed and illustrated through a set of design studies and explorations, this paper shows how these concepts may be used *analytically* to investigate issues such as privacy and security, *anticipatorily* to speculate about the future of technology development and use, and *generatively* to synthesize design concepts and solutions.

KEYWORDS: Design inquiry, research through design, critical HCI, privacy, surveillance, smart home, smart city, Internet of Things (IoT)

ACM Reference format:

James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *2019 CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland, UK.* ACM, New York, NY, USA. Paper 45, 14 pages. https://doi.org/10.1145/3290605.3300275

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300275

INTRODUCTION

In 2001, when asked about the possibility of a Google "implant" technology, then CEO Eric Schmidt responded by stating that "Google policy … is to get right up to the creepy line—but not cross it" [[19]]. In formulating this response, Schmidt sketches the contours of an important concept for engaging with social and ethical issues bound up with technology.

The metaphor of a creepy line implicitly frames a set of tensions by framing technology design, development, and use as an issue of *social acceptability.* On one side of the creepy line lie clearly useful, beneficial, and beloved technologies. On the other lie those deemed unacceptably scary, dangerous, or otherwise problematic. In framing creepiness as a line—a border or threshold past which technology is deemed *too* creepy—the notions of benefits, costs, harms, and tradeoffs enter into the picture.

This research project takes creepiness as a useful and provocative starting point for investigating a host of timely concerns at the intersection of people and digital technology, including privacy, security, trust, accountability, and fairness. This research takes creepiness as an entry point for conducting a design-led inquiry into smart technologies wherein the processes and outcomes of design are both a subject and method of inquiry. Broadly this research asks, How do the products of interaction design navigate, and perhaps even manipulate, shifting lines of creepiness and social acceptability? While this question is expansive, the focus is narrowed throughout this paper by focusing on a specific subject—smart home security cameras—and a specific unit of analysis—the interfaces and interactions of these products.

Through this design-led inquiry investigating the relationships between design and creepiness, this research develops three key concepts. *Digital leakage* names the propensity for digital information to be shared, stolen, and misused in ways unbeknownst or even harmful to those to whom the data pertains or belongs. *Hole-and-corner applications* are those functions connected to users' data, devices, and interactions yet concealed from or downplayed to them, often because they are non-beneficial or harmful to them. *Foot-in-the-door devices* are product and services with functional offerings and affordances that work to normalize and integrate a technology, thus laying groundwork for future adoption of features that might have earlier been rejected as unacceptable or unnecessary.

This paper develops these concepts with three types of usage in mind. These concepts can be used *analytically* to study people and technology, and to help formulate and investigate theoretical and empirically questions. These concepts can also be used *anticipatorily* to speculate about the future of technology. And these concepts may also be used *generatively* to explore interventions and directions for addressing and redressing creepiness and the social and ethical problems that creepiness registers and helps bring to light.

BACKGROUND

Entry Point: Creepiness and Related Issues

Creepiness relates to a collection of timely and critical topics including privacy, security, accountability, trust, and fairness in the context of digital and interactive technologies. No longer dismissible as buzzwords, within recent years these topics have solidified into important subjects of research and debate within HCI, academia, and public discourse. This research takes an oblique cut into this cluster of concerns by focusing on creepiness and lines of social acceptance of technology.

This research is not the first to explicitly investigate creepiness in a sociotechnical context. Within HCI, Shklovski et al. have drawn attention to the significance and prevalence of users' experiences of creepiness when tracked by their smartphones [[63]]. Building on this work, Pierce and DiSalvo isolate creepiness as pivotal "network anxiety" and use it as a "central node through which to connect and route other more troubling effects" [[57]:4].

Outside of HCI, academics have also focused on creepiness as both an empirical phenomenon and a theoretical lens. Tene and and Polonetsky, writing in the context of law and technology, present a "theory of creepy" which offers "strategies for avoiding creepiness without dampening innovation," including advocating for transparency and putting a burden on users to consider "the golden rule" [[66], p. 59-60]. Others have discussed creepiness in the context of educational technologies [[7]] and big data [[21]]. However, there appears to be little if any scholarship that specifically engages with creepiness at the level of the interface and interactivity, and from the perspectives of design.

Without naming creepiness directly, a much larger body of work has investigated related issues of digital privacy, security, trust, accountability, and fairness. Within HCI, privacy and security has formed an active area of research for decades [[23],[24],[25],[33]], although only within the past few years has the HCI design research community deeply engaged with privacy and security issues. Other active areas of research within HCI with ties to creepiness include cyberharrassment [[2],[9],[55]], data ethics [[65]], technology addiction [[67],[74]], and a range of investigations into smart homes, cities, and devices [[17],[27],[31],[38],[38],[45],[71]].

Focus: Smart Home Security Cameras

The emerging smart home and city is a rich and timely site to investigate creepiness. The much-hyped emerging landscape of IoT (Internet of Things) technologies has already introduced many consumers—often of affluent and tech-savy demographics—to novel modes of interaction and smart functionality. While there are many fascinating new devices to consider, this research focuses on one: *smart home security cameras*. These devices exemplify a new consumer technology delicately, if not precariously, balanced along a creepy line. On one side, these devices offer security against old and new threats to the home. On the other, they introduce new vulnerabilities by subjecting the most private and intimate interior spaces to tracking and surveillance. Hanging in the balance along this secure/creepy line, smart home security cameras are striking instances of and metaphors for the contemporary growing pains, tradeoffs, and anxieties that accompany bringing smart surveillant devices into the most intimate and private spaces of the home. The poetic valence is greatest with *indoor* smart security cameras, such as Amazon's Indoor Cloud Cam and Google's Indoor Nest Cam. Here, with the smart camera gaze literally pointed *at the self within the home*, a user may willingly subject oneself to 24-hour surveillance—and all for the purpose of increasing home security.

Approach: Design-Led Inquiry

This research practices a design-led inquiry that follows in the tradition of research through design approaches within HCI [e.g., [29],[77]]. This inquiry consists of carefully observing and analyzing existing design interfaces and interactions coupled with creating novel design scenarios and proposals. The concepts articulated in this paper have been developed *through* a research through design process involving design studies and explorations, many of which are not presented within this paper. The selection of design studies and explorations that are presented in this paper serve a second function of aiding to *illustrate* the concept presented, in addition to their original function as means of developing these concepts.

The inquiry practiced here most closely follows the author's prior work in collaboration with DiSalvo [[57]], and some of the ideas developed in this paper can be read as an extension of this prior work investigating network anxieties. Similar to prior work by Pierce and DiSalvo, this paper is influenced by approaches within the arts and humanities.

The design research methods, tactics, and perspectives pioneered and refined across many additional prior works have also informed the design-led inquiry practiced in this research. The use of the speculative design proposal [[56]] plays an important role in this research, particularly those reliant upon sketches, diagrams, and collage such as prior works by Gaver [[30]], Boucher et al [[11]], Hooker et al [[3]], and Blythe et al [[12]]. These design studies of design artifacts have been influenced in part by Hauser and Wakkary et al's post-phenomonological analysis [[34],[70]], and Wong and Mulligan's analysis of corporate concept videos [[75]]. This research further builds upon a nascent tradition of HCI research that skillfully integrates *humanities theory and criticism* with *research through design* [[43],[59],[57],[70]].

DIGITAL LEAKAGE

"Information wants to be free," goes the saying famous saying often attributed to Internet pioneer Steward Brand. Years later—with the Internet thoroughly privatized and financialized—the corollary to Brand's famous claim is that *digital data wants to leak.* Digital information is easily shared, stored, and used. And there is always someone who stands to benefit from leaking and using private information. *Digital leakage* names the propensity for digital information to be shared, stolen, and misused in ways unbeknownst and possibly harmful to those to whom the data pertains, originates, or belongs. Through processes of digital leakage, seemingly private or secure digital information is surreptitiously collected, shared with additional parties, and used in unexpected and unsolicited ways. Digital leakage occurs both accidentally and intentionally, as well as both openly and secretly. Examples of leakage are diverse, and include the use of personal data for targeted third-party ads, large-scale data breaches, illegal law enforcement surveillance of smart phones, and sharing sexually explicit personal content without consent [[18]].

As noted by Shklovski [[63]] and others, *leakage* is a common metaphor used in privacy and security discourses [e.g.,[37],[41],[44]]. This paper develops and extends this metaphor by focusing on sites and processes of digital leakage connected to interfaces and interactions. How does leakage occur, and where should we look for it? This research highlights three key sites of digital leakage: *leaky sensor fields*, *leaky data pipelines*, and *leaky data analytics.*

Leaky Sensor Fields and Smart Home Cameras

The nascent consumer IoT product category of smart home security cameras greatly expands the scope and capacity of leaky sensor fields. Smart products such as Google's Nest Cam or Amazon's Cloud Cam offer innovative new features. Many smart security cameras apply artificial intelligence (AI) to recognize and analyze human anatomy, behavior, and environmental activity. Smart alerts are another innovative feature of these devices that apply cloud-based analytics to notify users via their mobile device when certain types of activity are detected. For example, the Nest Cam can alert users when it detects an unfamiliar face, thinks it sees a person, or senses activity. In addition to analyzing video and audio data, some home security cameras carry sensing capabilities for detecting ambient light and device temperature [[48]]. These new technical innovations greatly expand the possibilities for leaky sensor fields.

This section presents a selection of design studies and explorations that shed light on the proliferation of leaky sensor fields into the most intimate and private everyday contexts. The first two design studies—*Leaky #CaughtOnNest Videos* and *Towards an Architectural Taxonomy of Leaky Camera Fields*—help us more concretely grasp the problems and issues at stake with leaky smart camera sensor fields. The third set of design proposals helps us imagine literal and metaphorical tactics for addressing leaky sensors with design.

Design Study: *Leaky #CaughtOnNest Videos*

The design and marketing of today's smart security cameras push the boundaries of conventional definitions of home security. An examination of marketing and advertising materials for Google's NestCam and Amazon's Cloud Cam, for example, reveals use cases that involve capturing candid and serendipitous snapshots of pets, children, and bizarre events—situations that extend well beyond the core use case scenarios of catching burglars or negligent caretakers. Google's "Best of Nest" platform

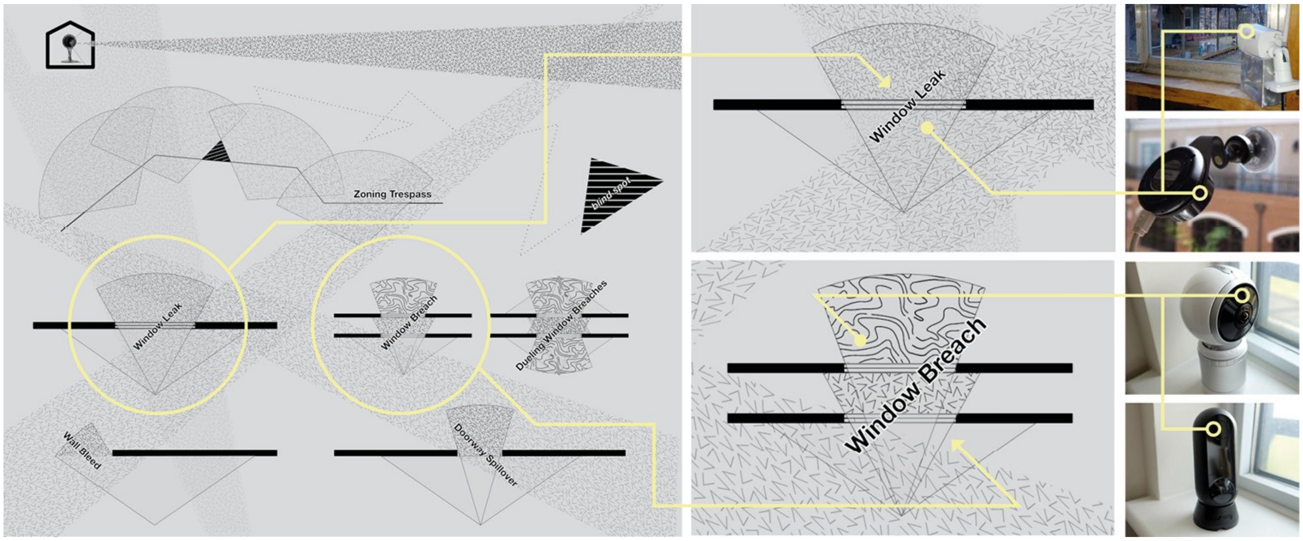


Figure 1. Towards an Architectural Taxonomy of Leaky Camera Sensor Fields

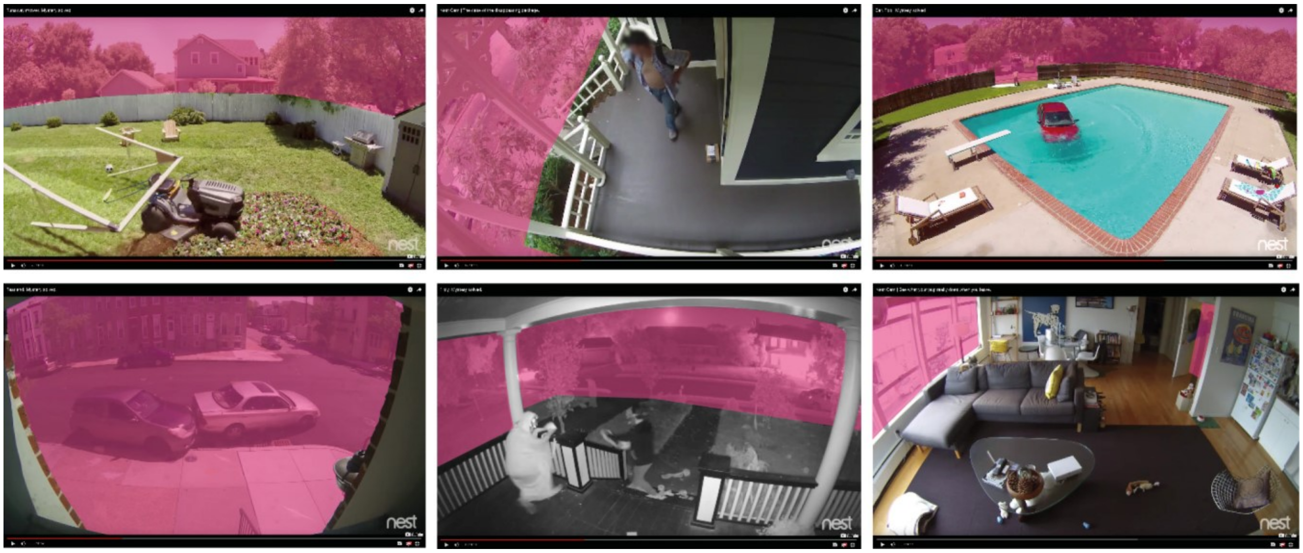


Figure 2. *Leaky #CaughtOnNest Videos.*

nurtures these extended uses by awarding the most captivating and entertaining videos caught on Nest [[49],[50]]. The site goes so far as to suggest a new, branded subgenre of social video—the Nestie.

In this design study (Figure 2) user submitted videos featured on the Nest website are modified to identify camera sensor leakage spilling over fences, property lines, and window and doorway thresholds. These studies draw attention to overlooked privacy and possible legal violations lurking in the background of these wildly entertaining and awe-inspiring moments #CaughtOnNest [[50]]. This analysis reveals potentials for leaky sensor fields to spread: to *drip*, *seep*, and *spill* over into previously unmonitored interstices and territories.

Design Study: *Towards an Architectural Taxonomy of Leaky Camera Fields*

The future of smart cameras may look something like this: As smart stationary cameras proliferate throughout public, private, and shared spaces, a sea of smart devices appear in formation to capture detailed data and produce analysis of bodily movement, searchable activity histories, and personal identity. In this scenario the surveillant leaky sensor field comes more clearly into focus. Leaky sensor fields form where the sensing capacities of smart cameras and similar devices cross socio-technical thresholds such as

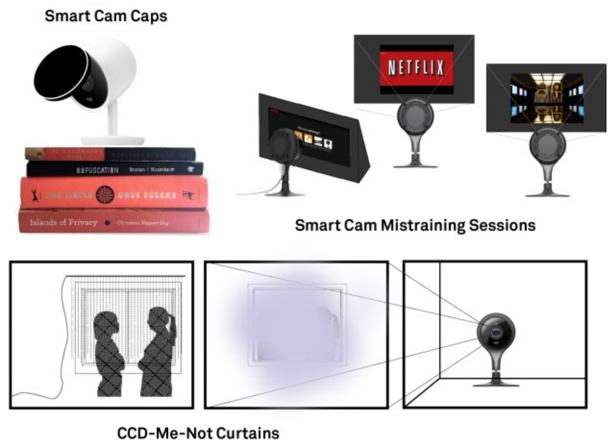


Figure 3. Design proposals exploring blindspots and noise as tactics for addressing digital leakage.

property lines, political boundaries, windowpanes, fences, and doorways. The inevitably pervasive leakiness occurring within neighborhoods and cities awash with smart cameras will provide ample opportunities for casual peeks into the lives of others, and for both open, feigned, and genuinely accidental surveillance of neighbors, friends, family, strangers, and ourselves.

This design exploration (Figure 1) aims to architecturally catalog and represent the emerging world of smart, leaky sensor fields. Consider, for example, the window breach where a smart camera is pointed at the window of a neighbor. The smart camera window breach does not simply allow someone to surreptitiously video record a neighbor. With a smart camera, someone can monitor the interior of neighbors home to automatically notify them when there is activity or when it identifies a certain or unfamiliar face. In the near future, a smart camera might easily peer into a neighboring window to tell you the occupant's mood, activity levels, and whom they have been keeping company with.

Design Proposals: Stopping Leakage with Blindspots and Noise

The two studies presented above illustrate specific sites and ways that leaky sensor fields operate: through windows, under doors, and in the overlooked background of images posted to social media. What is left out of the frame highlight an opportunity in combating leaky sensor fields: creating, maintaining, and leveraging sensor blindspots. *Sensor blindspots* form at the limits of a device's sensing capacities. Sensor blindspots can form at the absence of a sensing device, or can be actively produced with physical or electromagnetic interference. For example, consider the above scenarios of the window breach or window leak. In these scenarios, artistic provocations that confuse or evade facial recognition and digital camera sensors may actually soon prove practically useful in everyday contexts. For example, consider Adam Harvey's CV Dazzle digital camouflaging makeup [[35]], NSAF's HyperFace camouflaging scarf [[47]], and Mark Shepard's camera blocking CCD-Me-Not Umbrella [[62]]. A tactic closely related to the creation of blindspots, and illustrated by Shepard's CCD-Me-Not Umbrella, is to introduce data obfuscating noise—a tactic theoretically elaborated by Brunton and Nissenbaum [[13],[14]].

The three design proposals below further illustrate specific ways that the design tactics of creating blindspots and noise can be applied as a way to disrupt and block digital leakage. **Smart Camera Sensor Caps** offer a starkly simple mechanism for empowering and encouraging individuals to control leaky sensor fields. Unable to fully trust that smart devices are not sensing or transmitting data, device restraints that physically and visibly block sensors can provide assurance that sensors are not leaking. Inspired by Mark Shepard's camera-blocking CCD-Me-Not Umbrella, ***CCD-Me-Not Curtains*** showcase a domestic application for infrared LED light interference techniques to disrupt the peering smart camera of neighbors or passersby. Whereas Shepard's umbrella is best read as an artistic provocation for imagining near-term futures, the CCD-Me-Not Curtains place this speculation much closer to immediate useful everyday applications. Finally, ***Smart Cam Mistraining Sessions*** illustrate a speculative everyday application of data obfuscation. Research has shown that cyberattacks on the Nest camera could reveal when the camera detects motion, indicating someone may be home, even when the traffic is encrypted [[4]]. Reports that iRobot might share maps of customers' homes gleaned from data collected by the Roomba robotic vacuum spurred discussions about what information could be revealed through smart home devices [[4]]. As a data obfuscating practice [[13],[14]] smart camera mistraining sessions might help to foil attackers and sabotage intimate data collection. In this scenario, a smart camera is configured to watch Netfllix shows to introduce noise in any analytics used to predict user's behaviors.

HOLE-AND-CORNER APPLICATIONS

Leaky sensor fields expand the range and context of what data are collected, stored, shared, and analyzed. Next we consider hole-and-corner applications that capitalize on digital leakage. *Hole-and-corner applications* are actual or imminently potential applications connected to a user's data, device, and interaction yet concealed from or downplayed to them, often because they are controversial, do not offer them clear benefits, or may even be harmful to them. An illustrative example of a hole-and-corner application is when reports surfaced in 2017 that the domestic robotic vacuum cleaner Roomba was generating maps of users homes [[4]]. This led to speculation that the iRoomba company might sell these maps to advertisers or other third parties. This possible hole-and-corner application scenario was reported with alarmist headlines such as "Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder" [[39]] even though iRoomba assured customers it would not do so.

This example of iRoomba Map *potentially* selling maps of users homes highlights important aspects of hole-and-corner applications. First, hole-and-corner applications contrast with the *aboveboard applications* openly offered and advertised to consumers. Hole-and-corner applications are by definition not prominently advertised or advocated by manufacturers and service providers—perhaps owing to propriety reasons, because of fear of consumer or stakeholder backlash, or out of concern for legal repercussions. Consequently, identifying hole-and-corner applications often requires a degree of speculation based on available evidence and an assessment of technological possibility. Actual hole-and-corner applications are often verified through press leaks, or surface through hacks or edge cases that reveal activities not previously known or considered.

Hole-and-corner applications include, but encompass more than, instances of malicious theft or malpractice. Some of the most significant hole-and-corner applications to consider are those with large-scale and far-reaching negative impacts that come to light after a disastrous event or investigative bombshell, such as the Snowden revelations, Facebook and Cambridge Analytica scandal, or lawsuits surrounding the use of IMSI-catcher surveillance of mobile phones by law enforcement in the US.

In this section, several troubling hole-and-corner application areas that utilize digital leakage from smart cameras are first considered. This section concludes with some speculative hole-and-corner application scenarios specific to smart home cameras.

Smart Cam Hole-and-Corner Application Areas

Following Pierce and DiSalvo, this section elevates sensational, outlier examples—what they refer to as "troubling edge cases" [[57]:4-5]. Pierce and DiSalvo articulate a tactic of "drawing lines between center and edge" as way of connecting the mainstream with marginal and outlier concerns. The edge cases discussed here connect mainstream consumer applications with hole-and-corner applications of smart cameras for predictive policing, neuromarketing, social credit, and cyberharrasment.

The following sections provide a brief overview of the relevance of smart cameras to controversial applications in neuromarketing, policing, social credit, and cyberharrassment. Having established links between smart cameras, these hole-and-corner applications are then considered within everyday domestic contexts. Several examples are used to illustrate possible future hole-and-corner application scenarios, and also to suggest a method of generating speculative hole-and-corner scenarios by extending controversial "edge case" examples into new contexts.

Targeted advertising and neuromarketing. Targeting advertising and neuromarketing share an insatiable appetite for big data in order to construct user profiles, predict user behavior, and increase the efficiency and effectiveness of advertising and marketing. Targeting advertising is "a form of advertising where online advertisers can use sophisticated methods to target the most receptive audiences with certain traits, based on the product or person the advertiser is promoting" [[73]]. Neuromarketing "studies which emotions are relevant in human decision making and uses this knowledge to improve marketing's effectiveness" [[53]].

Two visually striking examples of the confluence of these two approaches were reported in a 2013 news article by Stephanie Clifford and Quentin Hardy [[20]]. RetailNext software uses video data to map customer paths throughout a store and differentiate men, women, and children's bodies while RealEyes software analyzes facial cues to assess customers reactions, emotional moods, and happiness levels.

Big data policing. Emerging techniques of predictive policing use big data and analytics to predict criminal activity. Andrew Ferguson writes of emerging "big data policing" scenarios, such as "real-time facial-recognition software that will link existing video surveillance cameras to massive biometric databases to automatically identify people with open warrants" [[26]:2]. The highly discriminatory and controversial potentials of these new systems were on full display in a 2016 academic paper titled "Automated Inference on Criminally using Face images." The authors used "supervised manual machine learning" of facial image data to "find some discriminating structural features for predicting criminality, such as lip curvature, eye inner, corner distance, and the so-called nose-mouth angle" [[76]:1]. News media was quick point to the racist eugenic evocations of the work [[8]].

Reputation and social credit. Big data and artificial intelligence are changing the operations and effects of prior reputation systems, such as government regulated credit scores. One of the most notable examples is the emergence of so-called social credit scores. While the British dystopian science fiction series *Dark Mirror* famously explored a disturbing future where social mistakes lower ones social standing, China is already implementing such systems. A prominent example is use of facial recognition to identify jaywalkers and shame them by posting their photos and docking social credit score [[10],[46]].

Cyber-harassment and Deepfakes. Cyberharrassment and cyberstalking are major social problems that social media, law enforcement, and legislators are still struggle to address. Danielle Citron has rigorously detailed how the Internet exacerbates the harms caused by conventional harassment and stalking by, for example, extending the life of destructive posts and exponentially expanding the reach of the harasser [[18]:3-4]. Cyberharrasment dovetails with another massive social problem that has emerged: fake news and digital misinformation. One particularly disturbing area that straddles fake news and cyberharrassment is deepfakes, or the application of deep learning to the production of fake videos. Deepfakes have launched an entire genre of fake celebrity and pornography videos. They have also enabled new forms of cyberharassment that laws have not caught up with [[15]].

Speculative Hole-and-Corner Scenarios

Predictive policing, neuromarketing, social credit, and cyber-harassment are four controversial application areas that utilize digital leakage from smart camera technologies. But how might these scenarios play out in the future smart home? *Speculative hole-and-corner application scenarios* is one method for answering this question. Each of the abbreviated use cases below involves a special case of hole-and-corner applications in which the owner of a smart camera subjects occupants and passersby to surveillance. Design use cases often revolve around a consensual, knowing user. The scenarios below instead center upon people such as children or guests with limited legal, social, or economic recourse to smart camera surveillance. Baumer more generally refers to this category as *usees*, "individuals who neither are clearly users of a system nor are clearly non-users" [[6]:1].

Design Scenario: *Catching the nanny being sad* (Figure 4). A domestic childcare worker is surveilled by her employer. Her behavior and emotions are monitored for erratic activity, signs of depression or anxiety, and job satisfaction. This scenario highlights a general hole-and-corner application area of *emotional domestic surveillance.*

Design Scenario: *Proving the neighbor keeps bad company*. A self-motivated citizen constructs a surveillance system to monitor their neighbor's guests' criminal records, citizenship status, religious affiliation, relationship status, and social media posts. This scenario highlights a more general hole-and-corner application area of *neighborly law and moral enforcement surveillance.*

Design Scenario: *Deep gaslighting a domestic partner*. A savvy and manipulative spouse uses deepfaked video and audio footage to convince their partner that *they* are the one with a history of emotionally abusive language—effectively implanting false memories into their partner's mind. This scenario highlights a more general hole-and-corner application of *digital gaslighting, blackmail, and false memory implantation.*

Using Speculative Hole-and-Corner Scenarios: Hole-and-Corner Subjects and Interior Profiles

One use of developing *speculative hole-and-corner scenarios* for designers, researchers, and policymakers is to anticipate or predict future developments, as scenarios are often used. Another use, however, is to extrapolate trends in order to better analyze and understand the present. With these scenarios, two considerations are highlighted which are often overlooked in design: *the hole-and-corner subject* and the *interior profile.*

In contrast to an informed and consenting user, hole-and-corner applications often involve unwitting, uniformed, or coerced subjects. A particularly illuminating user profile to consider is a domestic worker such as nanny, caregiver, or housecleaner who, in many countries, are excluded from worker protection laws. Oftentimes it is a hole-and-corner subject, rather than an informed, consenting, and benefiting user, who stands to lose the most or suffer the greatest harms resulting from creepy hole-and-corner applications.

The scenarios above further bring into focus a new development in the evolution of the user profile. User profiles are collections of data associated with a person that are used to construct models that can predict behavior. The speculative hole-and-corner scenarios and subjects above highlight the emergence of *interior profiles*: domestic profiles, household profiles, activity profiles, as well as other place-based profile. Some smart home devices such as

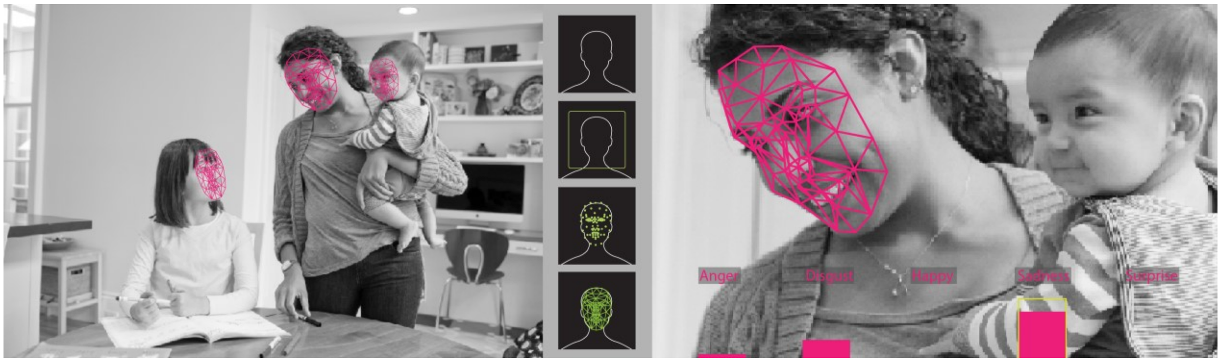


Figure 4. Catching the Nanny Being Sad. Emotion tracking can reveal when people are sad or depressed even when it is not apparent, or they themselves do not know.

Amazon Echo allow users to configure a household profile in addition to a user profile. While the collection, and leakage, of aggregated household data may provide anonymity, these profiles may also lead to models with greater individual predictive power and opportunities for disaggregation and de-anonymization.

The design scenarios presented here foreground the ways in which smart home devices may work their way into the most intimate corners, hidden crevices, and darkest closets of people's lives. The staggering amount of intimate data collected by these devices hold immense value to companies and their partners, and increasingly to law enforcement, credit bureaus, and government security agencies. As one reporter writes, "the [smart home] race is not just about selling fancy appliances. It's also a fight for which company coordinates smart homes and collects data about the habits of those who live inside." [[40]].

FOOT-IN-THE-DOOR DEVICES

Hole-and-corner applications operate surreptitiously behind the scenes and out of the spotlight. But unwelcome or unsolicited applications and features can also emerge slowly over time. This section develops the concept of *foot-in-the-door devices*—functional offerings and affordances that lay the groundwork for the future adoption and integration of features that might have been rejected previously as unacceptable or unnecessary. An illustrative example of a foot-in-the-door device is how the smartphone created opportunities for mass-scale, and in some cases illegal, surveillance by governments and corporations. Democratic citizens and informed consumers would not voluntary carry a device in their pockets whose sole function was to track their movement and activity without offering compensation or benefits. However, the form and functions of the smartphone created foot-in-the-door potentials—or, in this case device-in-the-pocket potentials—that were later exploited and capitalized upon. This example also highlights the challenge of assessing whether a retrospective foot-in-the-door analysis reveals strategic intent or foresight, or merely a series of emergent, largely accidental opportunities. Foot-in-the-door device is a useful concept for analyzing and anticipating how technologies develop and gain acceptance over time through a combination of incremental changes (small steps) and gradual changes (slow shifts). While design is often framed as an activity for solving problems and improving user experiences, the concept of a foot-in-the-door device emphasizes how design employs techniques with aims of persuading, manipulating, and obtaining compliance.

In social psychology, the foot-in-the-door technique is a compliance tactic where someone is persuaded to agree to a large request by first agreeing to a more modest request [[28]]. The underlying principle according to social psychologists is that the small request creates a social bond that makes them more likely to agree to subsequent requests—including those that they would have originally declined. First studied from a psychological perspective in the 1960s, the basic idea has been captured in much older sayings such as the fable of the camel's nose, the metaphor of a boiling frog, and the proverb of death by a thousand cuts. Foot-in-the-door differs from bait-and-switch because in the latter case the person baited eventually realizes they were defrauded, whereas in the former case any unwelcome effects are gradual.

The tradition of design has it own version of this technique. According to renowned American industrial designer Raymond Lowey, in order to sell something surprising, make it familiar. And to sell something familiar, make it surprising. Lowey famously captured this principle in the acronym MAYA: Most Advanced Yet Acceptable. According to MAYA, the ideal design is neither too strange nor too familiar, but rather sufficiently advanced and surprising while at the same time familiar and

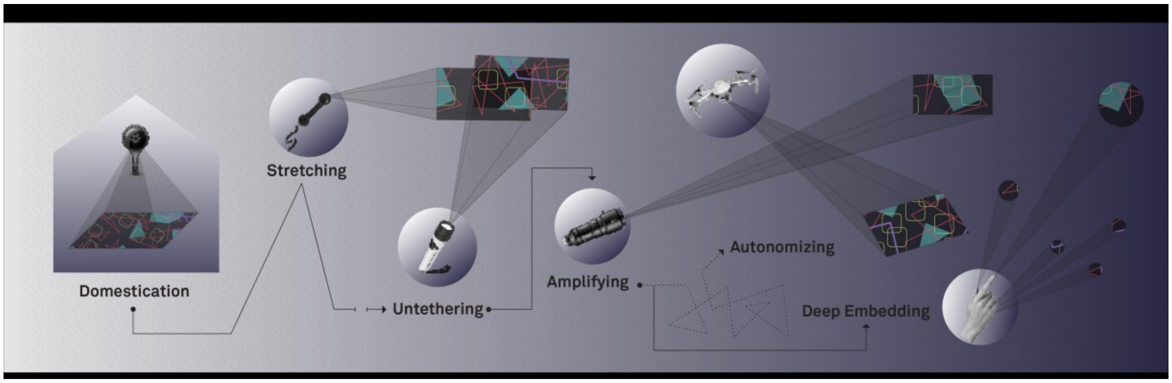


Figure 5. Smart camera speculative foot-in-the-door roadmap.

understandable. We see the principle of MAYA applied brilliantly in the design and marketing of today's smart products, notably with the smart phone. While the telephone functionality is among the least used native applications of today's smartphones, in marketing the smartphone as a *phone* the novel device is made legible, accessible, and palatable. A similar technique is at work in the design and marketing of smart watches, smart cars, and smart homes. The studies of smart home security cameras in this section lead to a refinement of MAYA: to sell something creepy, make it safe, recognizable, and only incrementally new and surprising. Today's smart home security cameras are an important contemporaneously unfolding case study in how foot-in-the-door persuasion techniques mix with MAYA principles of acceptability and desirability to manage and manipulate shifting creepy lines.

More than a Camera, More than a Security Device

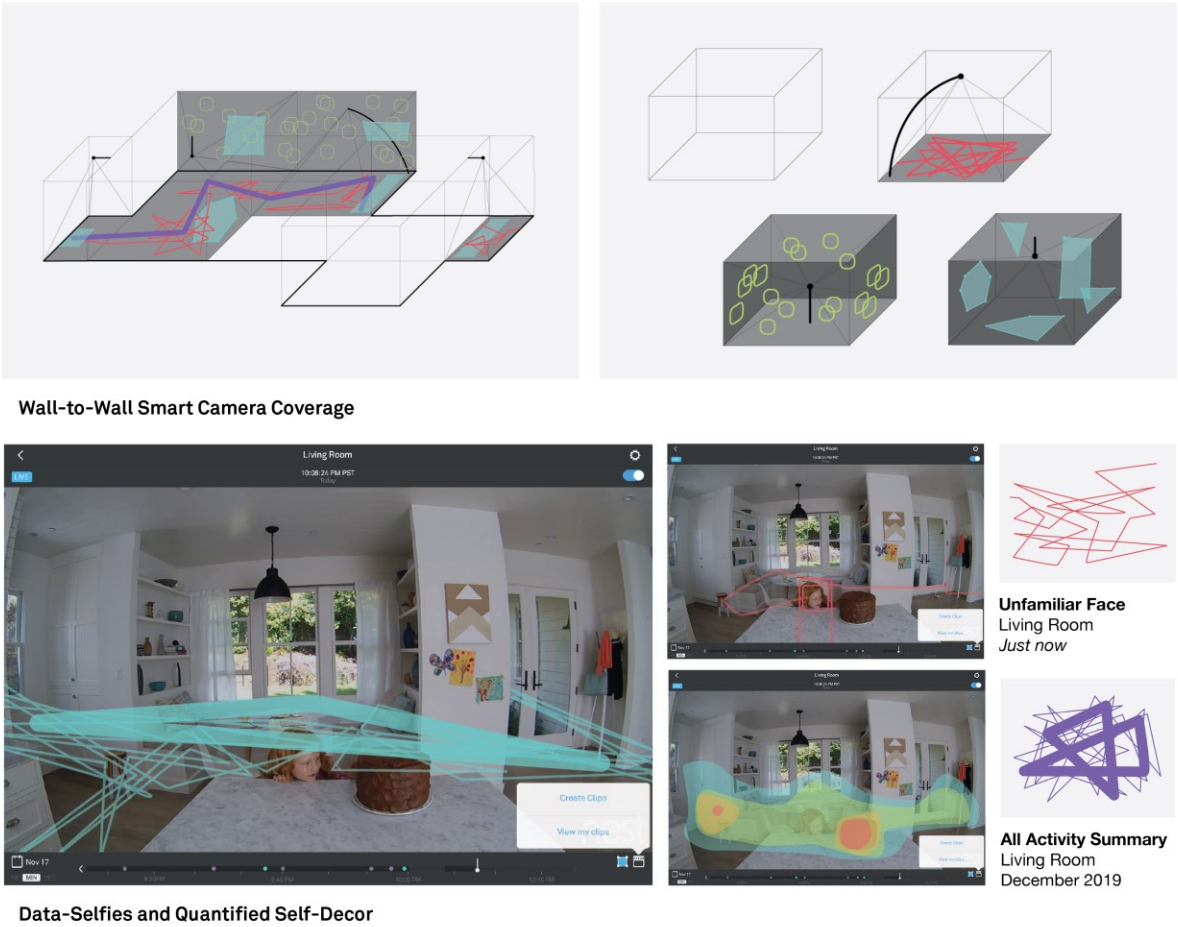
Reviewing the emerging landscape of smart security cameras through the filters of foot-in-the-door devices and MAYA reveals two key trends. First, *smart security cameras are technically much more than cameras.* Today's smart security cameras automatically alert users when motion or people are detected, they allow homeowners to view live camera feeds from their phones, and some even identify individual faces. And as with many smart products, security cameras such as Nest Cam collect environmental data including device temperature and ambient light [[48]]. Cloud-based subscription services such as Google's Nest Aware offer copious data storage and sophisticated data analysis. The most recent innovation is the Nest Cam's familiar face alerts, which comes with the caveat that "Depending on where you live, you may need to get consent to scan the faces of people visiting your home" [[48]]. Users may think they are buying a better security camera but are actually getting much more.

Second, *smart security cameras offer more than security.* The Nest Cam may be sold as a security camera, but its marketing materials often suggest it as a lifestyle or entertainment device with analogies to social media and handheld digital cameras. For example, Nest users are invited to submit their favorite videos captured with the smart security cameras [[49]]. Selected videos are posted on the Nest Videos webpage under categories that, in addition to "Security", include "Mystery Solved", "Family Moments", "Pets", "Nature", and "Timelapses." The best user submitted content is honored with "Nestie Awards" for categories such as "Best Dog in a Lead Role" and "Best Fall". Nest advertisements frequently feature pets and kids, suggesting a radically inclusive notion of "security." Users may think they are buying a camera simply for security, but ultimately it fulfills social, playful, and reflective functions.

Speculative Foot-in-the-Door Roadmaps/Scenarios

If smart home security cameras are foot-in-the-door devices, where might their creeping trajectory be heading? Given the shifts and expansions from classic security functions of catching home intruders and delinquent caregivers to capturing videos of pets and kids and living among books and furniture, the following abstract scenarios imagine a foot-in-the-door roadmap that extends the reach and functions of smart cameras within the home.

Stretching and Untethering. The static, fixed-length power cord lengthens and eventually detaches completely. Inspired by vacuum cleaners and landline telephones—task-specific devices designed to be put away after use—we consider scenarios for smart cameras with long, retractable cords and springy, coiled cords. Designs concepts explored include mobile standalone smart camera with a snap-off magnetic power charger and handle that is designed to float around home like a remote control or a toy, or be easily carried and ready at hand like a flashlight or mobile phone.


Wall-to-Wall Smart Camera Coverage

Data-Selfies and Quantified Self-Decor

Figure 6. Design proposals for *Wall-to-Wall Camera Coverage*, *Data-Selfies*, and *Quantified Self-Décor*.

Amplifying. Sensor amplification can develop in multiple directions: extended view angles, increased resolution, or additional sensing capabilities such as lidar or GPS. Concepts explored include a smart security camera retrofitted with a telescopic lens and directional microphone—possibly for a neighborly law enforcement surveillance scenario outlined previously.

Autonomizing. Once untethered, smart cameras may begin to robotically pivot, swivel, and rove. Autonomous movement further amplifies sensing capacities. Concepts explored include a Roomba-inspired roving camera and swarms of camera pocket drones.

Deep embedding. When miniaturization and wireless power are combined with untethering and amplifying, smart camera become deeply embedded into surfaces and objects. This embedding creates unprecedented opportunities for concealment, mobility, and extended reach. Concepts explored include smart camera embeddings into everyday objects and environments: a pen, a finger, a cat collar, a greeting card, a plumber's snake, a cockroach.

Imagining Foot-in-the-Door Trajectories in Finer Resolution

A new physical support infrastructure will be needed if smart home camera surveillance spreads into the most intimate and private spaces such bedrooms, tabletops, and closets. Developing a design analogy with electric lighting, a scenario is imagined where a variety of lamp-like supports are used to configure smart cameras and direct their gaze across different rooms, angles, and activities. Referencing the popularization of wall-to-wall carpeting, this scenario considers the emergence of a physical infrastructure for ***wall-to-wall smart cam coverage*** (Figure 6).

As an example of a more concrete user application built atop wall-to-wall coverage, several design proposals are used to imagine new genres of digital photography and home décor. ***Quantified self (QS) and quantified home (QH) Décor*** displays self-surveillance data for aesthetic and reflective uses without self-improvement or productivity in mind. **Data-selfies and auto-selfies** imagines a new types of social media posts enabled by wall-to-wall coverage (Figure 6).

DISCUSSION

Having introduced and illustrated each of the three key concepts, this final discussion section further elaborates each concept in two ways. The discussions that follow further connect each concept to additional prior research. The uses of each concept as analytic, anticipatory, and generative tools are further discussed by outlining future directions for their applications and by suggesting more general methodological frameworks for applying them.

Digital leakage, a recurring metaphor in privacy and security discourse, here names the propensity for digital information to be shared, stolen, and misused in unbeknownst or even harmful ways. As a corollary to the maxim information wants to be free, this paper has proposed that *digital data wants to leak*. This research has developed the concept of digital leakage through a process of putting design studies and explorations into dialogue with critical scholarship from media and technology studies. Tung-Hui Hu, for example, has proposed sewers as an alternative metaphor for reframing cybersecurity hygiene debates [[37]]. Shoshana Zubeff reveals how large technology companies strategically transformed trivial bits of *"data exhaust"* into entirely new and now dominant business models built around the collection of lucrative personal data [[79]:79-81]. This design-led inquiry has investigated leakage specific to smart security cameras and through this process shown how these devices are creating new openings for collecting intimate information. While the ostensive function of smart security cameras is to improve home security, the longer-term foot-in-the-door intents or effects may be to embed and normalize yet another leaky, lucrative data collection device within the most private and intimate of spaces.

This research has articulated three general sites at which smart technologies leak*: **leaky sensor fields**, **leaky data pipelines***, and ***leaky data analytics***. The concept of digital leakage is a useful metaphor for framing problems of privacy and security, and for identifying material causes and effects. Extending the metaphor of leakage—and building upon the data exhaust and sewage metaphors discussed by Zubeff and Hu—leads to additional concepts for findings leaks, assessing their harms, and formulating means of redressing them: digital leaks that ***drip*** and slowly accumulate, such as insurers collecting bits of seemingly trivial information; leaks that quietly and invisibly ***seep***, like IMSI-catcher mobile phone eavesdropping; pipes that occasionally burst and ***gush***, such as massive data breaches; and drips, seeps, and gushes that combine streams and ***pool*** over time.

In using digital leakage as a critical analytic concept, leakage should be understand as not simply a bug but also a feature of digital technologies. If we follow Zubeff's analysis, digital leakage is a mechanism deliberately built into the technical infrastructures and business models undergirding today's products, services, and platforms [[78],[79]]. At a broad level, digital leakage as a critical concepts provides a useful counter-narrative to the celebration of *sharing* as new digitally enabled experience and social value in its own right. Digital leakage is the dirty, ignoble flipside of sharing. At the level of interfaces, leakage provides a set of alternative interaction metaphors for diagnosing problems and generating solutions.

Hole-and-corner applications are applications connected to a user's device, data, or activity but that are concealed from or downplayed to that user. The concept of hole-and-corner applications provides a necessary handle for naming and grasping the gamut of parallel and shadow applications that contrast with the shiny features used to promote and sell technologies. In contrast with useful and seductive *aboveboard* applications, hole-and-corner applications are concealed because they offer no unequivocal or outweighing benefits, and may even be harmful.

As a method, this research demonstrated a technique of generating ***speculative hole-and-corner scenarios***. Speculative hole-and-corner applications can both anticipate and elevate troubling future scenarios downplayed or concealed by organizations, as well as playing a role in a sort of forensic analysis set on attributing intent or foresight, and thus culpability [c.f. [72]].

Foot-in-the-door devices are product and services with functional offerings and affordances that work to normalize and integrate a technology, thus laying groundwork for future adoption of features that might earlier have been rejected as unacceptable or unnecessary. The concept of a foot-in-the-door device emphasizes design as practice of persuasion, manipulation, and compliance.

As a method, this research has demonstrated a technique of generating ***speculative foot-in-the-door roadmaps***. As with the technique of generating speculative hole-and-corner scenarios discussed previously, foot-in-the-door roadmaps are useful tools for both anticipating future scenarios, regardless of evidence of intent, and for the task of constructing arguments making a case for strategic foot-in-the-door intent—an approach that aligns with Eyal Weizman's critical approach to *forensis* [[72]].

When analyzing how a technology operates as a foot-in-the-door device, there are two key aspects to consider. ***Small steps*** are incremental changes that are much easier to accept than more drastic, jarring ones. Small steps can lead to a *ratcheting incrementalism of normality*, as sociologist Elizabeth Shove has argued [[64]]. In the context of smart homes and cities, once a smart device is in the door—or in the pocket, on the wrist, or secured to a street post—it can be exceptionally difficult to toss them out, take them off, or tear them down. The close interaction studies of indoor smart security camera cords and bases have here revealed how small design details can play pivotal, and perhaps outsized roles in facilitating social acceptance and integration of technologies that might otherwise be considered much too creepy. ***Slow shifts*** are changes that happen gradually over time, rather than suddenly and all at once. Slow shifts can lead to imperceptible normalization. Jarod Diamond poignantly highlights this critical temporal dimension in his studies of civilizational decay and death caused by human-induced natural disasters. Adapting the term *creeping normalcy* used by politicians, Diamond writes: "If the economy, schools, traffic congestion, or anything else is deteriorating only slowly, it's difficult to recognize that each successive year is on the average slightly worse … so one's baseline standard for what constitutes 'normalcy' shifts gradually and imperceptibly" [[22]].

While foot-in-the-door devices and dovetailing tactics of MAYA, bait-and-switch, feature creep, and creeping normalcy are common, and effective, techniques employed by designers, they also raise ethical issues around consent, transparency, and control, and draw attention to unfair and harmful effects of the small steps and slow shifts quietly ushered in by foot-in-the-door devices

Conclusion: Expanding Our Vocabulary for Engaging with Social and Ethical Issues

This research set out to investigate shifting and retreating lines of creepiness in the emerging smart home by focusing on smart home security cameras. Through a process of closely analyzing existing design interfaces combined with generating novel design scenarios and proposals, this inquiry has developed and illustrated three key concepts: *digital leakage*, *hole-and-corner applications*, and *foot-in-the-door devices*. This paper has introduced these concepts and shown how they may be used *analytically* to understand relationships between interactive technology, user experience, and issues of privacy, security, trust, accountable, and fairness. These concepts may also be used *anticipatorily* and *generatively*, as this paper has shown, to extrapolate future trends and speculate about future possibilities, and to generate design interventions, solutions, and other design-oriented responses.

While this paper makes minor contributions with regards to analyzing, anticipating, and generating specific designs related to smart home security cameras, the core contribution is to develop and present new and refined vocabulary for understanding, discussing, and addressing timely social and ethical issues with smart technologies. This contribution builds upon and adds to theoretical, empirical, and critical scholarship that has proposed similar concepts for understanding issues such as privacy and surveillance—such as Nissenbaum's general theory of contextual integrity [[52]] and Zubeff's concept of surveillance capitalism [[78]]. The three concepts developed in this research, however, are distinct from those developed in prior research in that they both arise from and are directed toward design broadly and interfaces, interactions, and user experiences specifically. These concepts allow us to go beyond generally labeling certain events as creepy, as invasions of privacy, or as breaches of trust by focusing on specific mechanisms by which design and technology lead to negative experiences and outcomes. By expanding our vocabulary through concepts such as digital leakage, hole-and-corner applications, and foot-in-the-door devices, we increase our capacity as designers, researchers, and critics to concretely analyze, discuss, debate, and address the dizzying array of existing and emerging issues at hand.

ACKNOWLEDGMENTS

This work was supported in part by a grant from the Center for Long-Term Cybersecurity.

REFERENCES

[1] Akrich, Madeleine. "The De-Scription of Technical Objects," 1992.

[2] Ahmed, Nova, Sadd Azmeen Ur Rahman, Rahat Jahangir Rony, Tanvir Mushfique, and Vikram Mehta. "Protibadinext: Sensor Support to Handle Sexual Harassment." In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, 918–921. UbiComp '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2968219.2979133.

[3] Aipperspach, Ryan, Ben Hooker, and Allison Woodruff. "The Heterogeneous Home." In Proceedings of the 10th International Conference on Ubiquitous Computing, 222–231. UbiComp '08. New York, NY, USA: ACM, 2008. https://doi.org/10.1145/1409635.1409666.

[4] Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., and Feamster, N. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic. Arxiv, 2017. https://arxiv.org/abs/1708.05044

[5] Astor, Maggie. "Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared." The New York Times, January 20, 2018, sec. Technology.

https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

[6] Baumer, Eric PS. “Usees.” In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 3295–3298. ACM, 2015.

[7] Beattie, Scott, Carolyn Woodley, and Kay Souter. “Creepy Analytics and Learner Data Rights.” Rhetoric and Reality: Critical Perspectives on Educational Technology. Proceedings Ascilite, 2014, 421–425.

[8] Biddle, Sam. “Troubling Study Says Artificial Intelligence Can Predict Who Will Be Criminals Based on Facial Features.” The Intercept (blog), November 18, 2016. https://theintercept.com/2016/11/18/troubling-study-says-artificial-intelligence-can-predict-who-will-be-criminals-based-on-facial-features/.

[9] Blackwell, Lindsay, Jean Hardy, Tawfiq Ammari, Tiffany Veinot, Cliff Lampe, and Sarita Schoenebeck. “LGBT Parents and Social Media: Advocacy, Privacy, and Disclosure During Shifting Social Movements.” In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 610–622. CHI ’16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2858036.2858342.

[10] Boing Boing.“Chinese Jaywalkers Are Identified and Shamed by Facial Recognition, and Now They’ll Get Warnings over Text Message.” Boing Boing. Accessed September 17, 2018. https://boingboing.net/2018/03/28/chinese-jaywalkers-are-identif.html.

[11] Boucher, Andy, David Cameron, and Nadine Jarvis. “Power to the People: Dynamic Energy Management through Communal Cooperation.” In Proceedings of the Designing Interactive Systems Conference, 612–620. ACM, 2012.

[12] Blythe, Mark, Jamie Steane, Jenny Roe, and Caroline Oliver. “Solutionism, the Game: Design Fictions for Positive Aging.” In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 3849–3858. ACM, 2015.

[13] Brunton, Finn, and Helen Nissenbaum. Obfuscation: A User’s Guide for Privacy and Protest. Mit Press, 2015.

[14] Brunton, Finn, and Helen Nissenbaum. “Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation.” First Monday 16, no. 5 (2011).

[15] Chesney, Robert and Danielle Citron. “Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy? - Lawfare.” Accessed September 19, 2018. https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

[16] Cialdini, R.B.; Vincent, J.E.; Lewis, S.K.; Catalan, J.; Wheeler, D.; Darby, B. L. (1975). "Reciprocal concessions procedure for inducing compliance: the door-in-the-face technique". Journal of Personality and Social Psychology. 31: 206–215.

[17] Cila, Nazli, Iskander Smit, Elisa Giaccardi, and Ben Kröse. “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, 448–459. CHI ’17. New York, NY, USA: ACM, 2017. https://doi.org/10.1145/3025453.3025797.

[18] Citron, Danielle Keats. Hate Crimes in Cyberspace. Harvard University Press, 2014.

[19] Cole, Robert. Google Eric Schmidt - The Creepy Line (Edited). Accessed September 17, 2018. https://www.youtube.com/watch?v=mpmOL-MT5lQ.

[20] Clifford, Stephanie and Quenin Hardy. “Attention, Shoppers: Store Is Tracking Your Cell - The New York Times.” Accessed September 17, 2018. https://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html

[21] Cumbley, Richard, and Peter Church. “Is ‘Big Data’ Creepy?” Computer Law & Security Review 29, no. 5 (2013): 601–609.

[22] Diamond, Jared. Collapse: How Societies Choose to Fail or Succeed. Penguin, 2005.

[23] Das, Sauvik, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15), 1416-1426. https://doi.org/10.1145/2675133.2675225

[24] Egelman. Serge, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08), 1065-1074.: https://doi.org/10.1145/1357054.1357219

[25] Dourish, Paul and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. Human-Computer Interaction 21, 3: 319–342. https://doi.org/10.1207/s15327051hci2103_2

[26] Ferguson, Andrew Guthrie. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. NYU Press, 2017.

[27] Sarah E. Fox, Rafael M.L. Silva, and Daniela K. Rosner. 2018. Beyond the Prototype: Maintenance, Collective Responsibility, and Public IoT. In Proceedings of the 2018 Designing Interactive Systems Conference (DIS '18). ACM, New York, NY, USA, 21-32. DOI: https://doi.org/10.1145/3196709.3196710

[28] Freedman, J. L.; Fraser, S. C. (1966). "Compliance without pressure: The foot-in-the-door technique". Journal of Personality and Social Psychology. 4 (2): 195–202. doi:10.1037/h0023552

[29] Gaver, William. “What Should We Expect from Research through Design?” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 937–946. ACM, 2012

[30] Gaver, William. “Making Spaces: How Design Workbooks Work.” In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1551–1560. CHI ’11. New York, NY, USA: ACM, 2011. https://doi.org/10.1145/1978942.1979169.

[31] Giaccardi, Elisa, Nazli Cila, Chris Speed, and Melissa Caldwell. “Thing Ethnography: Doing Design Research with Non-Humans.” In Proceedings of the 2016 ACM Conference on Designing Interactive Systems, 377–387. DIS ’16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2901790.2901905.

[32] Goldschmidt, Gabriela, Hagay Hochman, and Itay Dafni. “The Design Studio ‘Crit’: Teacher–Student Communication.” AI EDAM 24, no. 3 (August 2010): 285–302. https://doi.org/10.1017/S089006041000020X.

[33] Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Risk-taking as a Learning Process for Shaping Teen’s Online Information Privacy Behaviors. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW ’15, 583–599. https://doi.org/10.1145/2675133.2675287

[34] Hauser, Sabrina, Doenja Oogjes, Ron Wakkary, and Peter-Paul Verbeek. “An Annotated Portfolio on Doing Postphenomenology Through Research Products.” In Proceedings of the 2018 on Designing Interactive Systems Conference 2018, 459–471. ACM, 2018.

[35] Harvey, Adam. “CV Dazzle: Camouflage from Face Detection.” Accessed September 17, 2018. https://cvdazzle.com/.

[36] Healy, John. “The Components of the" Crit" in Art and Design Education.” Irish Journal of Academic Practice 5, no. 1 (2016): 7.

[37] Hu, Tung-Hui. A Prehistory of the Cloud, 2015. Cambridge MA, MIT Press, 2015.

[38] Jenkins, Tom. “Cohousing IoT: Design Prototyping for Community Life.” In Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction, 667–673. ACM, 2018.

[39] Jones, Rhett. “Roomba’s Next Big Step Is Selling Maps of Your Home to the Highest Bidder.” Accessed September 17, 2018. https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829.

[40] Kopytoff, Verne. “The Real Reason Google Paid $3.2 Billion For Nest.” Time. Accessed September 18, 2018. http://business.time.com/2014/01/14/the-real-reason-google-paid-3-2-billion-for-nest/

[41] Krishnamurthy, Balachander, and Craig E. Wills. “Generating a Privacy Footprint on the Internet.” In Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, 65–70. ACM, 2006.

[42] Lentricchia, Frank, and Andrew DuBois. Close Reading: The Reader. Duke University Press Durham, NC, 2003.

[43] Liu, Jen, Daragh Byrne, and Laura Devendorf. "Design for Collaborative Survival: An Inquiry into Human-Fungi Relationships." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 40. ACM, 2018.

[44] Lin, Jialiu, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing." In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, 501–510. ACM, 2012.

[45] Lindley, Joseph, Paul Coulton and Rachel Cooper. Why the Internet of Things needs Object Orientated Ontology, The Design Journal, 2017.

[46] Ma, Alexandra. "These Are the Things That Can Get You Punished under China's Creepy 'social Credit' System — from Fake News to Jaywalking." Business Insider. Accessed September 17, 2018. https://www.businessinsider.com/china-social-credit-system-things-you-can-do-wrong-and-punishments-2018-4.

[47] Neurospeculative afro-feminism. "Nsaf." Accessed September 17, 2018. http://www.hyphen-labs.com/nsaf.html.

[48] Nest.com."Privacy Statement for Nest Products and Services." Nest. Accessed January 6, 2018. https://www.nest.com/legal/privacy-statement-for-nest-products-and-services/

[49] Nest.com."The Nestie Awards, Year Two | Nest." Accessed December 22, 2017. https://nest.com/blog/2017/03/08/the-nestie-awards-year-two/.

[50] Nest.com. "Video | Nest." Accessed December 22, 2017. https://nest.com/video/category/security/

[51] Nest. "Support." Nest. Accessed September 19, 2018. https://www.nest.com/support/article/.

[52] Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 2009.

[53] NMSBA. "NMSBA - What Is Neuromarketing." Accessed September 17, 2018. http://www.nmsba.com/what-is-neuromarketing.

[54] Oxford dictionary, "Creepy | Definition of Creepy in US English by Oxford Dictionaries." Oxford Dictionaries | English. Accessed September 17, 2018. https://en.oxforddictionaries.com/definition/us/creepy.

[55] Pater, Jessica A., Moon K. Kim, Elizabeth D. Mynatt, and Casey Fiesler. "Characterizations of Online Harassment: Comparing Policies across Social Media Platforms." In Proceedings of the 19th International Conference on Supporting Group Work, 369–374. ACM, 2016.

[56] Pierce, James. "On the Presentation and Production of Design Research Artifacts in HCI." In Proceedings of the 2014 Conference on Designing Interactive Systems, 735–744. ACM, 2014.

[57] Pierce, James, and Carl DiSalvo. "Addressing Network Anxieties with Alternative Design Metaphors." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 549. ACM, 2018.

[58] Pierce, James, and Carl DiSalvo. "Dark Clouds, Io&#!+, and [Crystal Ball Emoji]: Projecting Network Anxieties with Alternative Design Metaphors." In Proceedings of the 2017 Conference on Designing Interactive Systems, 1383–1393. ACM, 2017.

[59] Rosner, Daniela K., Miwa Ikemiya, Diana Kim, and Kristin Koch. "Designing with Traces." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1649–1658. ACM, 2013.

[60] Schön, Donald A. "The Architectural Studio as an Exemplar of Education for Reflection-in-Action." Journal of Architectural Education 38, no. 1 (1984): 2–9.

[61] Schüll, Natasha Dow. Addiction by Design: Machine Gambling in Las Vegas. Princeton University Press, 2012.

[62] Sheperd, Mark. "Sentient City Survival Kit." Accessed September 17, 2018. http://survival.sentientcity.net/umbrella.html.

[63] Shklovski, Irina, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. "Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use." In Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems, 2347–2356. ACM, 2014. http://dl.acm.org/citation.cfm?id=2557421.

[64] Shove, Elizabeth. "Comfort, Cleanliness and Convenience: The Social Organization of Normality (New Technologies/New Cultures)," 2004.

[65] Skirpan, Michael Warren, Jacqueline Cameron, and Tom Yeh. "More Than a Show: Using Personalized Immersive Theater to Educate and Engage the Public in Technology Ethics." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 464. ACM, 2018.

[66] Tene, Omer, and Jules Polonetsky. "A Theory of Creepy: Technology, Privacy and Shifting Social Norms." Yale JL & Tech. 16 (2013): 59.

[67] Vaghefi, Isaac, and Liette Lapointe. "When Too Much Usage Is Too Much: Exploring the Process of It Addiction." In System Sciences (HICSS), 2014 47th Hawaii International Conference On, 4494–4503. IEEE, 2014.

[68] Verbeek, P. P., and Slob, A., 2006, User Behavior and Technology Development: Shaping Sustainable Relations between Consumers and Technologies, vol. 20 of Eco-Efficiency in Industry and Science, Springer, Dordrecht.

[69] Verbeek, Peter-Paul. "Obstetric Ultrasound and the Technological Mediation of Morality: A Postphenomenological Analysis." Human Studies 31, no. 1 (2008): 11–26.

[70] Wakkary, Ron, Doenja Oogjes, Henry WJ Lin, and Sabrina Hauser. "Philosophers Living with the Tilting Bowl." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 94. ACM, 2018.

[71] Wallace, Jayne, Jon Rogers, Michael Shorter, Pete Thomas, Martin Skelly, and Richard Cook. "The SelfReflector: Design, IoT and the High Street." In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 423. ACM, 2018.

[72] Weizman, Eyal. "Introduction: Forensis." Forensis: The Architecture of Public Truth, 2014, 9–32.

[73] Wikipedia. "Targeted Advertising." Wikipedia, September 5, 2018. https://en.wikipedia.org/w/index.php?title=Targeted_advertising&oldid=858248415.

[74] Wisniewski, Pamela, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M. Carroll. "Resilience Mitigates the Negative Effects of Adolescent Internet Addiction and Online Risk Exposure." In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 4029–4038. ACM, 2015.

[75] Wong, Richmond Y., and Deirdre K. Mulligan. "When a Product Is Still Fictional: Anticipating and Speculating Futures through Concept Videos." In Proceedings of the 2016 ACM Conference on Designing Interactive Systems, 121–133. ACM, 2016.

[76] Wu, Xiaolin, and Xi Zhang. "Automated Inference on Criminality Using Face Images." ArXiv Preprint arXiv:1611.04135, 2016.

[77] Zimmerman, John, Jodi Forlizzi, and Shelley Evenson. "Research through Design as a Method for Interaction Design Research in HCI." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 493–502. ACM, 2007.

[78] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. (In Press: January 2019). Public Affairs.

[79] Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." Journal of Information Technology 30, no. 1 (2015): 75–89.