Addressing Network Anxieties with Alternative Design Metaphors

James Pierce
University of California Berkeley
Jacobs Institute for Design Innovation
Berkeley, California, USA
pierjam@berkeley.edu

Carl DiSalvo
Georgia Institute of Technology
School of Literature, Media, and Communication
Atlanta, Georgia, USA
cdisalvo@gatech.edu

ABSTRACT
Optimism and positivity permeate discourses of smart interactive network technologies. Yet we do not have to look too far or too deep to find anxieties knotting up on the horizon and festering below the network's glistening surface. This paper contributes a set of concepts, tactics, and novel design forms for addressing network anxieties generated through a design-led inquiry, or research through design approach. We present three technically grounded metaphors illustrated with examples selected from our exploratory design process. Weaving together concepts from surveillance studies, cultural studies, and other areas of the humanities with our visual and physical design work, we help draw attention to under-addressed concerns within HCI while proposing alternative ways of framing and engaging design issues arising with network technologies.

Author Keywords
Design Research, Internet of Things, Speculative Design

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
In a world where more and more things are found with power cables and batteries, sensors and central processors, unique identifiers and network connectivity—and where the people and entities that manage or are forced to remain offline may still find their images, geolocations, and other intimate data amid "the cloud"—what was once the Internet increasingly appears inseparable from digital technology broadly. *The network* (composed of networks, connected to networks) is a way of naming the proliferating multiplicity of smart technologies that lies somewhere between the historical Internet and digital technology in general. This network is wonderful. And it is overwhelming.

One way to grasp the network in its distributed and diffuse totality is to fixate upon its pivotal metaphors: a cyber-space, a virtual net, a surfable web, an information superhighway, a global village, a digital commons, a social web 2.0, and most recently a cloud and an Internet of Things (IoT). If there is a single message carried through this historical succession of metaphors, it is one of positivity. The network continues to make the world a better, smarter, more connected place to live. Its underlying mythology tells a tale of empowerment, freedom, choice, and opportunity. The network is not neutral. It has dominant and imposing values. And they skew positive.

And yet, belying its metaphorical positivity, we don't have to look too far or too deep to find anxieties knotting up on the horizon and festering below the surface of the network: A newly unveiled Microsoft AI (artificial intelligence) chatbot proclaims that Hitler did nothing wrong and feminists should burn in hell. Personal data from a Fitbit activity monitor bracelet is subpoenaed in a murder trial. The average U.S. adult spends 2 hours and 51 minutes on their phone and there is, of course, an app that will show a person how they compare to a statistical average. Laughter may be a natural response to network anxieties. As may deleting a social media account, taping over your laptop webcam, or retrofitting your bedroom with electromagnetic radiation blocking screens.

This paper contributes a set of design-oriented concepts, tactics, and forms to help address *network anxieties*. Based on our investigations into a diverse set of concerns—ranging from online privacy policies to police militarization to digital ghost detectors—we present three alternative design metaphors based on technical concepts from computing and networking: *troubling edge cases, pervasive fields,* and *unique personal identifiers*. This research sits at the intersection of HCI, the arts, and the humanities. We draw from theories and tactics from these fields, including at times the use of humor and satire, and we embrace a style of writing and visual communication that strives to be evocative and expressive. By drawing together concepts and perspectives from surveillance studies, cultural studies, and other areas of the humanities with our design work, we aim to draw attention to under-addressed concerns within HCI and to offer some specific design-oriented lines of future inquiry and intervention.

Negative Network Affects
Of particular focus for our investigations are network anxieties, a term that highlights the tensions between the clearly positive affective dimensions of network technologies and their often more hidden or marginalized negative affective dimensions. Defined as worry or unease concerning an "imminent event or something with an uncertain outcome," [1] anxiety names an experiential state of negative affect situated in anticipation of negative future outcomes. Anxiety—like the hopeful promise of new technology, or the imaginative projections of HCI and speculative design—is a future-oriented disposition. Our

 ACM ISBN 978-1-4503-5620-6/18/04\ ...\$15.00.
http://dx.doi.org/10.1145/10.1145/3173574.3174123

inquiry constructs a frame amid the visceral and other than fully rational or conscious forces [44] of *negative network affects*—of so many experiential breakdowns and perturbations that disturb the network's smooth edges and slick surfaces. Network anxieties manifest where lurking and looming disturbances poke through and put pressure on the network's smart shiny exterior, interrupting and troubling otherwise productive, convenient, and pleasurable interactive experiences. When this happens, negative affect collides with and perforates and perhaps overwhelms the network's generally positive disposition. Underlying the real joy, pleasure, and prosperity of network technologies one can often locate more hidden or marginalized feelings of discomfort, fear, frustration, distrust, paranoia, overstimulation, exhaustion, and creepiness.

Serious inquiry into the negative effects of technology is often eclipsed by an approach to technological design and development that exudes hope and optimism and, consequently, obscures the more disturbing and distasteful aspects of technology. Constructing a frame of inquiry around negative network affects allows for sustained consideration of a wide range of the more troubling impacts of HCI, IoT, and AI within a broader field that tends to embrace the positives and downplay the negatives. In some cases network anxieties signal more worthwhile and pressing problems than those ostensibly solved by the technologies that produce them. Whenever a smart fridge is hacked and spammed [23,49] or the packets for a $400 smart juicer are easily squeezed by hand [52], one cannot help but wonder if technology is addressing the right problems or merely creating unnecessary ones, or worse. In considering a range of negative network affects and their corresponding sources and effects—from the mildly amusing to the seriously and dangerously alarming—this paper seeks to provide concepts and tools for designers and researchers to address complex and emerging social and ethical concerns with new network technologies.

Of course, not all network anxieties are equal, nor or their underlying causes or distribution of material effects. While the most violent and harmful effects of networks are not felt equally by everyone, network anxieties seem to pop up everywhere—in headlines, on social media feeds, within pop culture and entertainment, during casual conversations and everyday interactions. Our strategy is to identify some under-addressed anxieties beneath the surface and at the margins of mainstream HCI, IoT, and AI research in order to trace them to their effects on the ground and just over the horizon. Naming and giving form to network anxieties can help ensure the right problems are addressed and attended to, a process aligned with what Mariam Fraser calls "inventive problem making" [11] and which Mike Michaels has extended in the realm of research through design [38, p. 542].

It is perhaps worth clarifying that our selection of specific concerns and examples within this paper is informed by our own biases and blind spots. The investigations we frame here are primarily informed by our selective triangulation of journalistic reporting, scholarly publication, and engagement with participants and interested parties. In this paper we do not report on the participatory and interventionist aspects of this research, instead focusing on conceptual framings and interpretations of design work in dialogue with secondary research and reporting. While the specific anxieties named and framed within this paper may resonate with some researchers and designers and perhaps help inform future lines of inquiry and intervention, for others it may be our broader approach and concepts that are of use in framing future work and catalyzing discussions.

Poised at the cutting edge of new digital applications, the fields of HCI and design research have shown a readiness to address problems and issues that arise with new interactive and networked technologies. These include issues of privacy [28,34,48], overload [33,39], digital civics [3], agency and choice [26,45], online labor [29,30], and new methods for an emerging IoT landscape [21] . Other issues such as the neoliberal construction of the user [23,27], gendered and racialized surveillance [7,12], and the weaponized violence of network technologies [31,32] have received comparatively scant attention within HCI.

Following lines of critical discourse within HCI and the humanities, our project is one of naming and giving form to network anxieties in ways that might help us confront, alleviate, and resolve them. In a word, our task is to inventively *address* network anxieties. Addressing has two key meanings. It can mean to locate and name. And it can mean to work to resolve and fix. This project begins by focusing on locating and naming as a means toward resolving and fixing.

Give Form to Network Anxieties through Design

One way of addressing networking anxieties is to give them imaginative and aesthetic form through design. The methods and approaches of design hold powerful yet relatively underutilized capacities for inventively addressing the very sources of network anxiety that they play such an instrumental role in producing. These capacities shine within the specialized approaches of speculative design, design fiction, critical design, and other alternative and critically-oriented design practices now common in HCI [e.g., 6,39,43,53]. Design's unique position to inventively address network anxieties stem from its ability to give vivid and graspable form to imaginative and compelling, if troubling, future possibilities. These forms distinguish themselves from other modes of knowledge production through their powers for understanding issues in highly concrete and contextualized ways, inviting participation and engagement from diverse stakeholders and constituents, and inspiring and generating creative affirmative responses. As an interface, design can connect the everyday buttons, handles, and screens with broader and deeper problems and issues. In some cases design may offer a solution or resolution, or else a fresh look or inspiring take on a difficult problem. In others, design may reveal its own limitations and point to the need other approaches.

Design-led inquiry is often characterized as a highly exploratory, emergent, and experimental process [e.g., 18]. In our experience with it, we typically don't know what we are creating or how to articulate its specific uses until we are well along in the process. Schematically, our process is one of designing and making things grounded in a set of timely concerns while iteratively reflecting on what we have created. Through this process two key questions emerged. First, *can we locate general sources, conditions,*

or states of network anxieties based on our design-inquiry and informed by critical thought from HCI and adjacent areas such as surveillance studies, media theory, and sociology? Second, *what specific, design-oriented concepts and tactics can we derive for addressing network anxieties* and interrelated issues tangled up with technology?

In response to the first question, we offer three technically grounded metaphors for addressing network anxieties, each arrived at through a process of clustering our distributed network of examples, sketches, diagrams, proposals, scenarios, use cases, analytic and generative frameworks, and other designerly forms. *Edge cases* address anxious network relationships that connect margin and center, outlier and norm, glitch and regularity. *Pervasive fields* address the atmospheric and all-encompassing, yet often imperceptible nature of network infrastructure. *Unique personal identifiers* address the ability of networked entities to be targeted and found, and the paranoia and fear this engenders. Each concept is extracted from the logics and technical discourses of network protocols, architectures, and infrastructures but then extended into the social and experiential domains and repurposed, with a critical edge, as diagnostic and generative tools for design and HCI.

Method: Projecting and Packeting Network Anxieties

This paper makes a secondary methodological contribution to HCI design research by synthesizing a unique combination of visual and physical design work. Our blending of elements from critical, speculative, and participatory design approaches involved generating a large set of visual design work while selectively augmenting this work with light-weight physical designs directed toward participatory and interventionist modes of engagement. We refer to these forms as design projections and design packets.

Our *design projections* allow us to explore a breadth of ideas in parallel through predominantly visual forms. Design projections draw from a rich design tradition of sketches, diagrams, collage, and conceptual proposals. Importantly our design projections are not limited to the genre of design proposal, which following Gaver could be succinctly defined as "a unitary vision of a proposed system's future" [18]. Instead many of our projections employ forms such as diagram, collage, and illustration oriented toward analytic or generative functions (see [40] for an earlier discussion). Formally and functionally, our projections take inspiration from design workbooks [18], design fictions [6,35], speculative design and architecture proposals, Constructivist and Dadaist collage, and the visual frameworks and diagrams commonly used in design planning, innovation, and human-centered design.

Our *design packets* allow us to selectively manifest and continue to explore our projections in a more interventionist and participatory manner. Our design packets channel the readymade, corporate schwag, DIY zines, physical sketches, and design probes. Formally our packets are designed as lighter-weight, smaller-scale, often single-use and ideally inexpensive forms [41]. The material, interventionist, and participatory dimensions share much in common with approaches such as speculative enactments [13], material speculation [53], cultural probes [20], the anti-art art of Fluxus, and diary and camera studies [25]. Here we focus on conceptual analysis, and reserve empirical reporting on our packet work for the future.) Our

Figure 1. *Smart Things (Creepy Vibes)*

design packets take inspiration from packet-switched networks and the splitting of complex data into manageable packets, but with an analog twist.

SMART APPY THINGS WITH REAL CREEPY VIBES

The smart home and smart city, rendered "intelligent" by cloud-enabled, uniquely identifiable IoT (Internet of Things) devices, are ideal sites to investigate network anxieties. The enticing product packaging of so many smart things—from coffee makers to sex toys to security cameras to toothbrushes—act as buffers between two versions of the smart home and city. Sealed inside and depicted on the surface lies an idealized, utopian-tending version. On the other side—unboxed, properly configured (we hope), and in-use—lie objects and interfaces of a "real world" smart home and city, complete with breakdowns, glitches, and less-than-ideal use cases. Among these negative network affects emanating from the smart home and city, one stands out: creepiness.

Shklovski et al. have recently highlighted creepiness as a key concept for HCI associated with network technologies, tracing connections among creepiness, the body, and potential or actual violations of personal space and information [46, p. 3]. If creepiness is taken as a pivotal negative affect associated with networked everyday things, then how do we characterize the idealized core or picture-perfect backdrop against which network creepiness periodically rattles and resurfaces? We propose two key qualities that contrast with network creepiness: smartness and appiness. *Smartness*, from a technical perspective, denotes a device that is connected (via wireless protocols to other devices or networks) and to some extent interactive and autonomous. Smartness describes a functional interior, the working core beneath the blinking lights and multi-touch screens. *Appiness* describes the experiential surface of so many smart devices. Smooth swipes, soft pings, and gentle buzzes are appy. So are single recessed buttons, automated wireless pairings, casual voice commands, minimal displays, and biCapped brandings. Appiness

Figure 2. *Network Anxieties Timelines and Coloring Books*

describes the interactional textures and countours of today's emerging suite of smart devices. In Figure 1 we diagrammatically distill out interactional textures of smart appy things, this serves as a guiding framework for our design-led inquiry, functioning as a central node through which to connect and route other more troubling effects. While qualities of smartness and appiness kindly shield us from computational and infrastructural complexity, they also mask creepy vibes and lurking edge cases. We turn next to traverse these edge cases and their troubling affects.

EDGE CASES

In engineering jargon, an edge case is an overlooked or underestimated case occurring at extreme operating parameters. For example, a driverless car may mistake a billboard depicting cyclists as actual humans and respond, much to the driver's dismay, by activating the breaks. Edge cases by definition are impossible to fully anticipate or prevent. This, coupled with possibilities of negative effects ranging from unpleasant to disastrous, and compounded by the scale and complexity of networks, invests edge cases with anxiety-inducing potential.

Reconfigured as a metaphor grounded in the technical engineering term, the edge case becomes a powerful concept for inventively addressing network anxieties. Doing so requires the edge case's expansion from a troubling engineering phenomenon, wherein it is treated as a technical problem awaiting a solution, to a troubling social and experiential phenomenon. Understood as socio-technical events, troubling edges cases are lingering blips, glitches, and anomalies in an otherwise smoothly functioning system that affectively disturb and effectively, if but momentarily, destabilize its center. This center—in actuality a mobile, evolving, and socially negotiated construct—represents core uses, operations, and norms associated with a network technology. Consider an example: In the immediate wake of a 2017 terrorist attack in London, the prices for the ride-share service Uber surge to 2.1 times the baseline rate [50]. Uber suspends the surge pricing within the hour, but the swift social media backlash prompts news headlines highlighting the controversial pricing algorithms undergirding the ride-sharing service.

Not containable to their outlier origin and status, nor easily written off as mere statistical anomalies or crackpot conspiracy theories, viral edge cases like the one above spread into the middle of a public discourse. Here they circulate and linger because of their power to call into question or validate concerns about their center. In the example above, the troubling edge case does not randomly fall from the sky but rather takes root within preexisting concerns, namely that technology companies have designed discriminatory algorithms to exploit workers, monetize all social interactions, and reap profit from situations that might otherwise engender solidarity and altruism. Cutting wider and deeper than mere technical glitches, troubling edge cases disturb and unsettle their smart, appy cores.

The remainder of this section explores troubling edge cases in greater resolution with the help of a selection of our design projections and packets. We use these examples to illustrate the concept of the troubling edge case, its relevance to inventively addressing network anxieties, and its utility as a diagnostic, anticipatory, and generative tool for design and HCI. Towards the goal of elaborating the concept of troubling edge cases we enumerate a number of troubling center/edge relations, such as concerns that exceptional disturbing instances might someday morph into newly sedimented norms. Towards the goal of presenting the troubling edge case as a design tool we outline tactics that involve reconfiguring center/edge relations.

Amplifying Edge Cases

An early stage of our process was to identify sources of network anxiety and collate them in digital and physical notebooks. *Network anxieties timelines* (Figure 2) represents one set of projections translating these anxieties. These timelines represent a more troubled, creepy version of typical Internet history timelines and infographics.

Our commitment to supplementing our visual design projections with participatory and interventionist design packets led us to translate sections of our notebooks into physical booklets. Intrigued by the surge in popularity of adult coloring book often promoted with stress therapy and mindfulness benefits, we experimented with this form as a way to softly trigger and perhaps help alleviate network anxieties. The spread in Figure 2 shows one of our more successful applications of the coloring book genre. Making

Figure 3. *Find My ____p_*

use of the non-digital and offline affordances of coloring books, these pages invite the reader to hand color Facebook Like icons. These coloring interfaces function as both a reminder of and momentary respite from network overstimulation, exhaustion, creepiness, and paranoia resulting from too much time spent refreshing feeds, liking posts, and avoiding targeted personalized ads.

A technique underlying the above compositions involves selecting, amplifying, and connecting edge cases. This leads us to design tactic of *giving amplified and interconnected form to edge cases*. This tactic works to address a core troubling center/edge relationship, namely that *edge cases remain at the edge, hidden from a concerned public eye, excluded from participation in a center, and left unaddressed and unaddressable*. Selectively amplifying troubling edge cases pushes them into the spotlight for consideration, debate, and, perhaps, affirmative response.

Drawing Parallels between Center and Edge

The adoption and integration of smart technologies for policing formed a key cluster of edge cases that emerged within our timelines and notebooks. This cluster of edge cases connects to broader trends and controversies concerning police surveillance and militarization across many areas of the world. Via a simple augmentation of our textural experience framework for smart appy things, *Smart Homes/Smart Policing* (Figure 3) traces connections between everyday smart devices and policing technologies. For example, The Starry Station Wi-Fi router, which emphasizes styling and easy of use, is paired with the StingRay Gemini 3-3, a controversial, and possibly illegal, surveillance device that intercepts mobile phone communications by mimicking cell towers. The Nest Smart Thermostat is paired with ShotSpotter, an environmental sensor that monitors gunshots. The Fitbits activity-tracking bracelet is connected to an Electronic Ankle Bracelet for monitoring individuals paroled or under house arrest.

This projection neatly illustrates a strategy of *drawing lines or parallels between center and edge*. It also shows how the concept of a troubling edge case is provocatively applied with metaphorical distance, extending the edge case from a technical concept to a social one. For example, here electronic ankle bracelet monitors for paroled individuals are rendered as edge cases of smart, appy activity bands. This strategy of connecting centers and edges highlights another troubling center/edge relation: the concern that *edge cases are excluded, distanced, obscured, or cut off from a smart appy center*.

In drawing explicit lines between smart appy consumer applications and specialized technologies of incarceration and domestic surveillance, Smart Homes/Smart Policing further invites a reading through the lens of racializing surveillance articulated by Simone Browne as "technology of social control where surveillance practices, policies, and performances concern the productions of norms pertaining to race and exercise a 'power to define what is in or out of place'" [7, p. 16, citing 15]. Smart Homes/Smart Policing provides an interactionally focused frame within which to consider how technologies "rationalized through industry specification and popular entertainment provide a means to falsify the idea that certain surveillance technologies and their applications are always neutral regarding race, gender, disability, and other categories of determination and their intersections" (p. 128). Figure 4 further evokes Hu's concept of the sovereignty of data through which "the cloud places users uncomfortably close to the mechanisms of state violence," suggesting how "[users] are in fact partially complicit with a violence that fails to respect boundaries between real and virtual space" [27, p. 115].

Extrapolating Edge Cases into Future Centers

Using Smart Homes/Smart Policing as a generative design framework, we produced a series of speculative design proposals that explore future scenarios of consumer-facing policing applications. Envisioned with an appy experiential texture, *Curfew* is a third-party smartphone app designed to help parolees and house arrestees comply with the terms of their sentence and thus avoiding prison incarceration by keeping appointments, meeting curfews, and staying clear of exclusion zones. *Find Offenders* uses a public crime API to display the whereabouts of criminal offenders sentenced to electronic ankle bracelet surveillance. *Crimecast* takes this concept further, leveraging crime data along with offenders' personal data to create forecasts predicting the likelihood of specific types of criminal activity such as robberies, assaults, mass shootings, and terrorist attacks.

These design proposals for future smart policing apps illustrate a tactic of *extrapolating edge cases out into a*

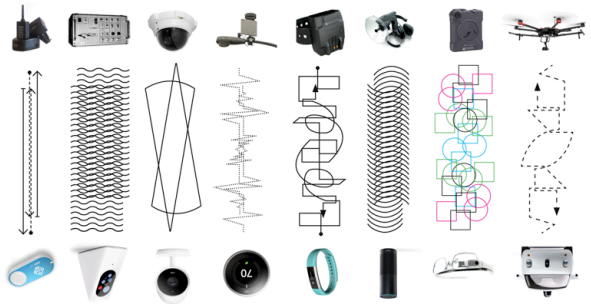

Figure 4. *Smart Homes / Smart Policing*

future center. They are rooted in the troubling center edge relation that *the edge might slowly creep or suddenly erupt into the center*. Extrapolating the present out into a troubling future is a core technique of dystopian science and speculative fiction, and of critically-oriented speculative design, where often a goal is to use projections of the future to understand and diagnose the present. Here we connect this technique to network anxiety-inducing edge cases treated as potentially alarming precursors of the troubling future centers and cores of daily life.

Renderings Edges as Centers and Vice Versa

Apple's native app Find My Friends allows people to view the location and track movement of friends and other contacts in real-time. In *Find My* _____ (Figure 3) we explore other scenarios for tracking the location and movement of acquaintances and strangers. Essentially we take creepy and disturbing, although to many not unfamiliar use cases and reconfigure them as the core functionality of an app. Of interest here are the ways in which the marketing of new digital technologies conceals and glosses over unpleasant, creepy, controversial, and sinister use cases.

Find my ____ illustrates a strategy of *re-centering the edge case to reveal its actual proximity*. Here it can be seen as a swap. We simply swap the advertised usage of finding friends with creepier use cases: stalking an ex, harassing women, tracking employees. This projection foregrounds another troubling edge/center relation: *that edge cases lie closer to the center than they might initially appear*.

Addressing Edge Cases

As a technically grounded metaphor, the edge case names a generalized source of network anxiety. Here we have outlined a set of tactics for tracing, amplifying, and reconfiguring troubling center/edge relations, and illustrated these tactics with a set of examples connecting emerging smart home technologies with technologies supporting state-sanctioned domestic surveillance, incarceration, and violence. Our brief case study demonstrates how these tactics may find use as diagnostic, anticipatory, and generative tools for design and HCI when it comes to addressing complex and possibly repressed negative network affects/effects associated with technology.

One of the dangers immanent within these tactics of tracing and amplifying edges cases is the potential for overstated and aestheticized forms to become confused with objective truth claims. Instead, it is crucial that we craft and use selectively amplified and aestheticized edge cases **not** as definitive evidence or alarmist propaganda, but rather as suggestive and exploratory forms. We might understand them as what Eyal Weisman calls *weak sensors* whose material aesthetic forms function to "register political forces", obfuscated and denied by dominant narratives, in ways "suggestive, rather than conclusive." [55, p. 29].

PERVASIVE FIELDS

Circulating as today's most pronounced and permeating metaphor for the Internet, "the cloud" signals a network expansion from tethered hubs of access via the terminal ends of cables to a substantially more ubiquitous and atmospheric connection. Scholar Tung-Hui Hu traces a "prehistory" of this nebulous "cloud," convincingly showing how modern network infrastructures of fiber optic cables and server farms are "grafted" onto older networks of railways, highways, military bunkers, and telephone lines [27]. Yet while their sources, as Hu argues, do in fact remain rooted in a sedimented infrastructure of tubes, boxes, and cables, these days the bits and bytes of networks have left the ground to radiate out into the atmosphere. Dreams of pervasive and ubiquitous computing, so imaginatively projected by HCI researchers in the early 1990s [54], were finally capable of large-scale realization with the implementation of a vast wireless infrastructure of cell towers and GPS satellites connected to smaller, localized systems of Wi-Fi routers and smart phones. The key enabling technologies were in the field of wireless communication. The pervasive wireless communication fields of network technology that include LTE, GPS and Wi-Fi are scientifically modeled as electromagnetic waves, or EMFs. Unlike the physical infrastructure of cables and towers, which are composed of atoms, EMFs are composed of photons, packets of energy imperceptible to the naked eye and to the bodies of most humans.

Pervasive fields, as a technically grounded metaphor for understanding network anxieties, address the atmospherically penetrating and all-encompassing yet often imperceptible nature of contemporary network infrastructure. Our bodies augmented with mobile network-enabled devices, these days sending and receiving data within the pervasive cloud of digitally-encoded waves can feel about as natural as breathing in and out. No longer tethered to cords and cables, our data (though technically waves of energy) hang in the air like atomized particulate matter waiting for a device-organ to detect and use it. But like an outbreak of airborne pathogens into the air, the ubiquitous fields of contemporary digital networks also harbor deeply troubling potentials among their life-improving applications.

At their best, pervasive network fields are useful, pleasant, and delightful—like breaths of fresh air or a single white cloud figured against a bright blue sky. At their worst, pervasive fields operate like airborne contagions, smog pollution, and chemtrail conspiracy theories: they instill or exacerbate feelings of extreme vulnerability and powerlessness. What defines the cloud when working at its best is also what can feel so troubling: it is everywhere, all the time, whether we want it or not. The problem with pervasive fields is that one cannot escape them, has limited ability to control them, and cannot directly perceive them.

To elaborate upon pervasive fields as a general source and condition of network anxieties, we first discuss *Ghost/Bug/Wave Detectors*, a set of design packets that probe relationships between the paranormal, surveillance, and electro-pollution. We then shift to a selection of projections that illustrate a more affirmative strategy of

Figure 5. *Ghost/Bug/Wave Detectors* product packets.

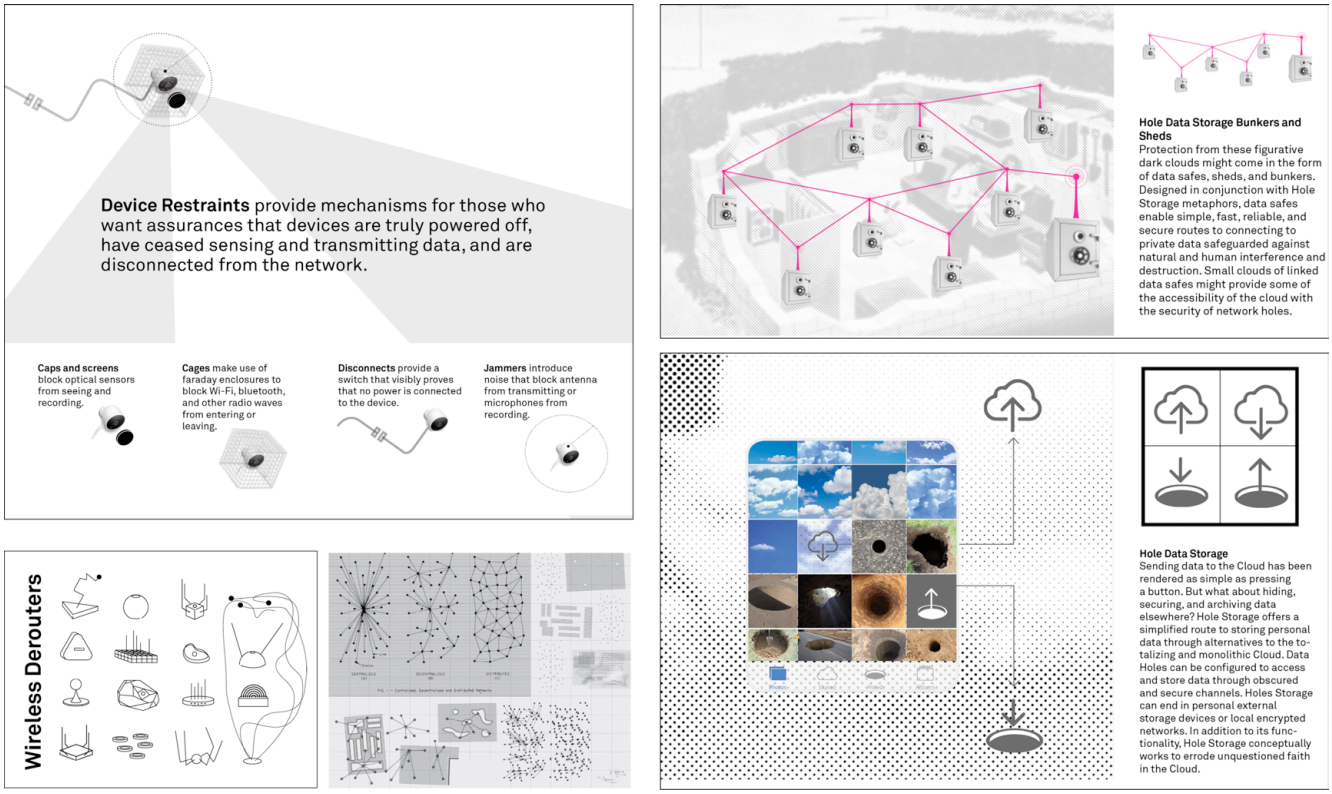

Figure 6. *Device Restraints, Wireless Derouters and Models for Digital Disconnectivity,* and *Hole Data Storage*

making holes in pervasive fields.

Ghost/Bug/Wave Detectors

Electromagnetic field (EMF) meters are tools originally designed for scientific and engineering purposes. Yet with the rise and spread of pervasive fields of network connectivity, these devices have developed new uses and meanings. Today EMF meters are also sold as tools to detect paranormal activity, electronic harassment and surveillance devices, and harmful radiation exposure. The existence of these rebranded and reappropriated devices register a curious entanglement of fringe and perhaps paranoid concerns often outright dismissed by mainstream scientific, medical, scholarly, and journalistic communities. Through these electronic sensing technologies, the ordinary pervasive electromagnetic fields—emitted by everything from phones to power lines to human and celestial bodies—are interpreted as evidence of ghostly hauntings, marks of conspiratorial electronic harassment, and artificial environmental causes of electrosensitivity, a physiological condition characterized by neurological and immunological symptoms in response to EMFs [4]. For us, the experience of seeing a ghost meter rebranded as a bug detector sold alongside an electro-pollution sensor, all arrayed via an Amazon recommender algorithm, was like picking up an unusual, eerie signal and wondering if it is a deliberate transmission or merely noise—a strange coincidence registering upon a vibrant, pervasive sea of electromagnetic waves. Whatever the explanation, the surprise meeting of ghost, bug, and wave detectors forms an exemplary instance of the sorts of creepy and unnerving possibilities lurking within the pervasive fields of networked experience.

Reflecting on the techniques at work within Ghost/Bug/Wave Detectors, two design tactics emerge for addressing network anxieties. First, they function as *fringe detection devices* for scanning fields and registering troubling fringe phenomena. Second, they operate through *careful entangling* of signals, particularly weak, noisy, and fringe detections. Both tactics offer routes to engaging with fringe beliefs, ghostly encounters, and conspiracy theories not necessarily as truth, but rather as "weapons of the weak" and disempowered [51, p. 143], and as ways in which "abusive systems of power make themselves known and their impacts felt in everyday life" [22 p. xvi].

Making Holes in the Network

A recurring signal picked up by our Ghosts/Bugs/Wave Detectors was a desire to escape from EMFs. This led us to a tactic of *making holes within pervasive fields*. A selection of design proposals illustrates this tactic below (Figure 6).

Hole data storage is a simplified route to storing personal data securely in a manner that never touches the cloud of corporate and government owned servers. Here the concept is portrayed on equal footing with ubiquitous cloud storage services like Google Drive, iCloud, and Dropbox. *Digital Quiet Zones and Wireless Derouters* enable or enforce the construction of digitally disconnected spaces that restrict or disable access to specific frequencies such as wifi, bluetooth, LTE, GSM, and GPS. While offering security against surveillance and hacking, digitally disconnected spaces are also explored as places to unplug and escape network distractions in order to concentrate, relax, converse, or contemplate. (This concept was originally explored in [42].) *Device Restraints* provide a variety of

Figure 7. *Digital Crystal Balls and Algorithmically Self-Fulfilling Prophecies*

measures for those that want assurances that devices are truly powered off, have ceased sensing and transmitting data, and are disconnected from the network. *Caps* limit the visibility of camera lens. *Cages* employ faraday enclosures to block Wi-Fi, bluetooth, and other radio waves from entering or leaving. *Disconnects* provide switches that visibly proves that no power is connected to the device.

Addressing Pervasive Fields

Today's network has left the ground and taken flight into the atmosphere, rapidly becoming as natural and necessary as the air we breath. Yet the pervasive utility and joy that rains down from the cloud is, upon closer inspection, full of anxieties rooted in the network's all-encompassing, often imperceptible, and increasingly inescapable fields. As one set of tactics for addressing the negative affects associated with pervasive fields we proposed *fringe detection devices* and *careful entangling* as ways of registering marginal concerns and marginalized experiences. As a way of generating more affirmative design responses, we have also illustrated a tactic of making holes in pervasive fields. This tactic readily links up with approaches advocated by activists, artists, and scholars such as obfuscation [8] and counter-surveillance [36,37]. While aesthetically provocative and well-matched to the processes and forms of design, such modes of tactical resistance present some important limitations and blind spots to consider, particularly in the context of HCI and design research. One is the tendency for anti-surveillance art, design, and activism to focus on product-based and individualized solutions, often for a universal subject that ignores categories such as gender, race, class, and disability [36,37]. While we have argued that the literal interfaces of technologies form a powerful metaphorical interface for grasping, understanding, and diagnosing complex socio-technical issues, when it comes to developing affirmative solutions it may prove more appropriate and effective to think and operate at the scales of policies, infrastructure,

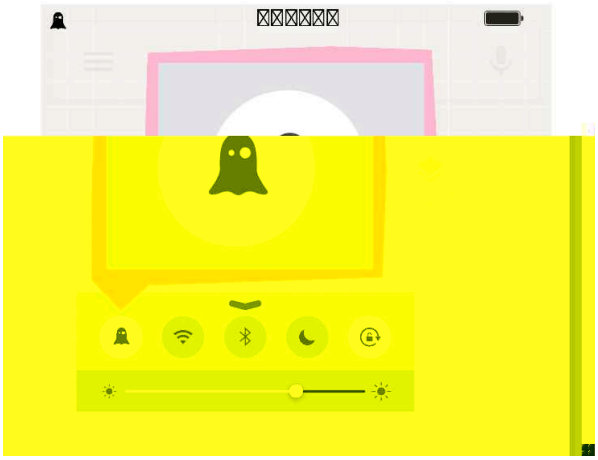

Figure 8. *Ghost* Mode

legislation, institutions, and social movements instead strictly focusing on the more focused and manageable scale of creating individual products and services. A second critique of the resistant, hole-making tactics favored by counter-surveillance activists and artists highlights the ways in which these tactics often mimic and reproduce those of the institutions which they seek to confront and disrupt, thus potentially "reanimating the very structures of power they purport to expose or overturn" [27, p. xxix].

Nonetheless, if today's dominant metaphors of the Internet project a world where everything is connected, holes within the connective pervasive fields can operate as a powerful metaphor for exploring alternatives.

UNIQUE AND PERSONAL IDENTIFIERS

Sometime around 2008 the network surpassed a noteworthy threshold: for the first time, more "things or objects" were connected to the Internet than people [14, p. 2]. Some experts have predicted that by 2020 the number of IoT devices will exceed 30 billion. The ultimate vision of an Internet of Things is that everything—including people, pets, cars, chairs, coffee machines, street signs, and bridges—is assigned a unique identifier that allows it to be addressed by and communicate over the network.

From a technical networking perspective, crucial to realizing this vision is the implementation and assignment of Unique Identifiers (UIDs) such as webpage URLs (Uniform Resource Locators), laptop MAC (media access control) addresses or IP (Internet Protocol) addresses. Formally, a unique identifier is a numeric or alphanumeric string that, from a technical perspective, enables networked entities to be addressed and thus accessed and interacted with. For example, the Mac address of this computer:

179.19.354.9[1]

Processed through the affective filter of network anxieties, the numerical precision and starkness of the UID deciphers into a creepy message:

You are being tracked, targeted, analyzed, manipulated.

[1] This UID has been altered to protect the privacy of the authors.

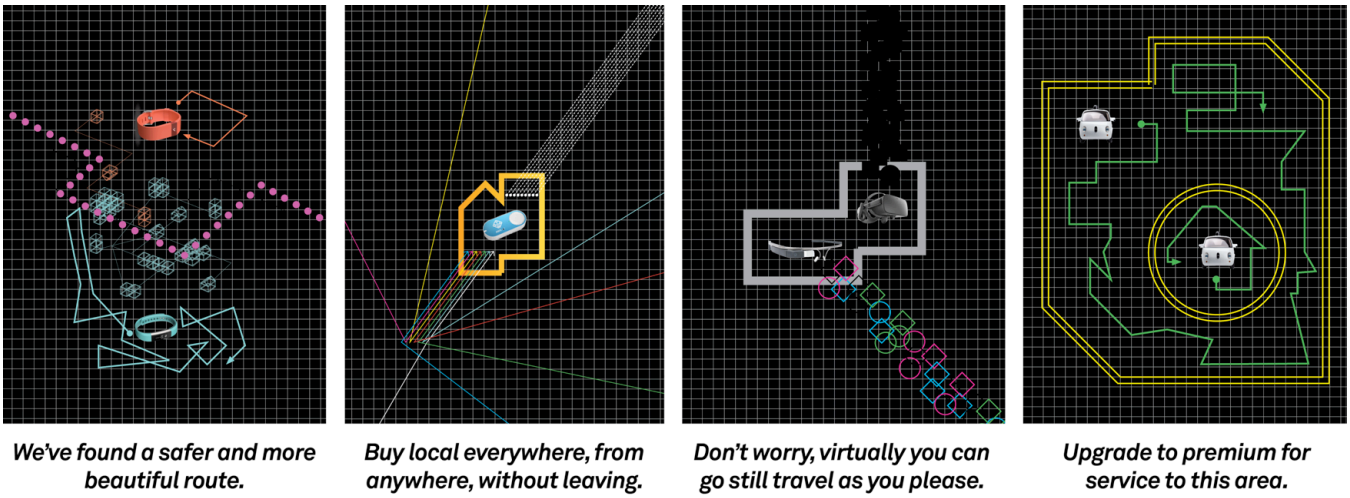

Figure 9. *Soft Exclusion and Confinement Zones*

Exacerbated by the rise of wearables, environmental sensors, implants, and biometric devices, and coupled with big data and machine learning algorithms, increasingly the network and those who operate, control, and infiltrate it know not only where *you* are but what you are doing, your preferences and proclivities, needs and desires, fears and anxieties—the network may even know you better than you know yourself [9]. As a metaphor, *unique personal identifiers* address the ability of networks to intimately track, target, analyze, and manipulate individuals, and the paranoia, fear, and unease this may induce.

Personalized Targeting, Analysis, and Manipulation

The useful applications that UIDs enable are profound, spanning from webpages and hyperlinks to GPS navigation and automated recommendations. But there are, of course, also troubling implications of world in which every person, place, and thing is assigned a set of unique identifiers. One is the ability for any entity to be targeted and found. Another is that the data uniquely associated with an entity is consequently subject to algorithmic analysis and manipulation. Below we present two scenarios that explore the paranoia, fear, and creepiness of UIDs.

Soft exclusion and confinement zones (Figure 9) considers everyday scenarios in which digital services use location and other personal data to restrict geographic movement, strategically position bodies, and construct and reinforce geopolitical and socio-cultural borders. In contrast with hard exclusion or confinement zones enforced with technologies such as border checkpoints and electronic ankle monitoring bracelets, soft exclusion and confinement zones operate more subtly, such as a ride share service offering price disincentives for travel to particular areas, or an app recommending restaurants or jogging routes based on biometric, financial, and social media data. These design projections evoke Gilles Deleuze's famously prescient example of a control society in which "people can drive infinitely and 'freely' without being at all confined yet while still being perfectly controlled" [11, p. 18].

Digital Crystal Balls and Algorithmically Self-fulfilling Prophecies (Figure 7) explore the fusion of search, prediction, and recommendation algorithms with fortune-telling, mind-reading, and prophecy. The scenarios portrayed here consider futures where personal recommendations and predictions are so irresistible or reputable that they manifest reality. If vast amounts of personal data coupled with machine learning algorithms generate personal predictions and recommendations that are almost always accurate, we might begin to assume they know where we should go, what we should purchase, or whether we are happy before we even view the results.

UID Transparency, Opacity, Translucency, and Mosaic

A common way of addressing network privacy issues surrounding UIDs is to create systems for network transparency built on the assumption that users can make more informed choices about personal privacy if the options and implications are made clear. The tactic of UID transparency is explored in several proposals below.

Inspired by so-called "right to explanation" arguments in the regulation of algorithms, *ARE (Algorithm Result Explanation)* depicts scenarios in which digital services offer users some transparency concerning how searches, recommendations, and predications are calculated and what data are used in the calculation. *Personal Data Reports, Privacy Facts Labels, and Monitoring Warning Labels* explore analogs to personal credit reports, nutrition fact labels, and alcohol and tobacco warning labels. As design interventions at multiple scales, these proposals explore combinations of information visualization, metrics and standards design, and legislation and policy. *Privacy and Data Policies in Print and Terms* of *Terms of Service Flashcards* are participatory and interventionist design packets that give more tangible, accessible form to the legalese encapsulated in browse-wrapped and click-wrapped agreements. The reception of these packets draw attention to limits of informed participation and usable privacy approaches. Many participants found some of the content alarming and disconcerting, yet did not take any direct action in response.

An opposite tactic attempts to render opaque the lenses through which personal data is collected in order to conceal and disrupt algorithmic analysis. Brenton and Nissenbaum refer to this approach obfuscation [8]. One way we have been exploring tactics of obfuscation is inviting people to use existing techniques popular with hackers and activists yet often inaccessible or unappealing to a general public. For example, *Dumb Burner Phone* packets invite people to use prepaid mobile phones to evade surveillance and increase privacy. A different approach involves projecting obfuscating tactics into the future. For example, a scenario of normalized obfuscation is explored in *Ghost Mode* (Figure 8), which takes the place of airplane mode after all personal electronics gain approval for use during commercial flights. Ghost Mode offers silent, invisible, untraceable activity and movement throughout networked space. When a device in Ghost Mode is probed or threatened, rather than fleeing it introduces noise and entropy in an attempt to thwart and corrupt data collection.

As an alternative to the extremes of either informed opt-ins or absolute opt-outs, we conclude with two examples that suggest tactics of translucency and mosaic. *Premium Privacy and Opt-Out Markets* envisions scenarios where the monetary value of personal data is openly displayed by presenting users with options to effectively sell or buy out of the collection of particularly invasive use of UIDs (e.g., selling a night of sleep data or an entire day of mobile phone and laptop camera access). *Personal Data Manipulators* imagines a social media or search feature that allows users to customize their personal data used to filter information, effectively allowing them to adopt the data profile of their true or ideal self, or someone else entirely.

Addressing Unique and Personal Identifiers

In response to the unease, fear, and paranoia that unique personal identifiers can induce, we have illustrated two opposing tactics—one of *transparency*, which aligns with usable privacy and security approaches, and one of *opacity*, which aligns with resistant tactics of counter-surveillance. Both tactics tend to figure a user as an individual subject empowered to act and either opt in to the logic and subjugation of networks, or else attempt to opt out.

If we follow Deleuze's influential treatment of how control societies operate, then the modern user figures not as an indivisible subject but rather as a dividual—a body divided up into "samples, data, markets" [11, p. 6]. The dividual helps illuminate the impossibility of total privacy or fully opting out. The dividualization of users into "life signatures" [1] and "data doubles" [23] further foregrounds the potential penalties and dangers from too much opacity, such as remaining invisible to friends or employers, or suspiciously incomplete to authorities or potential partners.

As an alternative to the extremes of full transparency or opacity, we suggested tactics of *translucency and mosaic*. Following Hu, "if we are not able to escape the throes of network fever"—the desire to connect everything—"then we might as well take pleasure from its deviances" and adopt joyful, improvisational, and transgressive ways of interacting within networks [27, 23, 11-24]. Or, following Wendy Chun against a misdirected desire to achieve network invulnerability, we might instead assume a position of vulnerability from which to "seize a freedom that always moves beyond our control, that carries with it no guarantees but rather constantly engenders decisions to be made and actions to be performed" [10, p. 30].

CONCLUSION

This paper has contributed a set of concepts, tactics, and design forms for addressing network anxieties. We began by framing a territory of negative network affects within which to inventively find, frame, and create problems associated with network technologies. Framing our inquiry around negative network affects directs us toward affective forces rather then easily quantifiable or statistically significant network effects. Our use of this term "network affects" engages in intentional semantic slippage between psychological affect, or emotion, and philosophical theory of affect as visceral and vital forces extending beyond emotion that "drive us toward movement, toward thought and extension, that can likewise suspend us (as if in neutral) across a barely registering accretion of force-relations, or that can leave us overwhelmed by the world's apparent intractability." [44, p. 1] For our task of addressing network anxieties, we are drawn to affective registers for their capacity to spark imagination and propel us through overwhelming feelings of intractability toward the inventive framing and making of problems.

The designs presented here, an RtD contribution in their own right, illustrated design tactics that help operationalize the design metaphors of **edge cases**, **pervasive fields**, and **unique personal identifiers**. These tactics are tools that others may use to address network anxieties by inventively framing problems or by affirmatively crafting responses. These tactics also function to reveal the thinking behind our own research through design process, responding to calls to demystify and explain design practice in HCI [5,43,47,57],

Design metaphors have a rich history within HCI. The alternative metaphors we've presented—grounded in technical networking discourse but redirected toward the negatively affective—help us see constructs such as clouds, smart homes, and personal digital assistants as metaphors by critically imagining alternatives (fog, cages, and spies, perhaps.) If we indeed want to address network anxieties along with other unwelcome aspects of interactive technology, we may well need new metaphors to do so.

Finally, we hope that we have also contributed to the corpus of work that employs theories and methods from the humanities and arts to HCI. One way we sought to do so in this paper is to offer an approach to thinking and writing that is open and lively, that does not attempt to come to quick resolution, but rather endeavors to be generous and generative. We approached our making activities similarly, drawing inspiration from arts practices such as tactical media, social practice, and art intervention to provide a space for creative inquiry that is both playful and sincere.

ACKNOWLEDGMENTS

This work was partly supported by National Science Foundation grant #1523562 and Intel. Although this paper does not present specific findings or outcomes of our engagements with participants and others, we nonetheless thank all of the people who spoke with us and engaged with our work. Thank you for generously sharing your time, thoughts, and stories, and for the inspiration, insight, and motivation you provided.

REFERENCES

1. Amoore, Louise. The Politics of Possibility: Risk and Security beyond Probability. Duke University Press, 2013.
2. "Anxiety | Definition of Anxiety in English by Oxford Dictionaries." Oxford Dictionaries | English. Accessed September 15, 2017. https://en.oxforddictionaries.com/definition/anxiety.
3. Asad, Mariam, Christopher A. Le Dantec, Becky Nielsen, and Kate Diedrick. "Creating a Sociotechnical API: Designing City-Scale Community Engagement." In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 2295–2306. ACM, 2017. http://dl.acm.org/citation.cfm?id=3025963.
4. Symptoms of EMF http://www.weepinitiative.org/areyou.html
5. Bardzell, Shaowen, Jeffrey Bardzell, Jodi Forlizzi, John Zimmerman, and John Antanitis. "Critical Design and Critical Theory: The Challenge of Designing for Provocation." In Proceedings of the Designing Interactive Systems Conference, 288–297. DIS '12. New York, NY, USA: ACM, 2012.
6. Blythe, Mark, Kristina Andersen, Rachel Clarke, and Peter Wright. "Anti-Solutionist Strategies: Seriously Silly Design Fiction." In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 4968–4978. ACM, 2016.
7. Browne, Simone. Dark Matters: On the Surveillance of Blackness. Duke University Press, 2015.
8. Brunton, Finn, and Helen Nissenbaum. Obfuscation: A User's Guide for Privacy and Protest. Mit Press, 2015.
9. Carmichael, Jessica. "Google Knows You Better Than You Know Yourself - The Atlantic." Accessed September 16, 2017. https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/.
10. Chun, Wendy Hui Kyong. Control and Freedom: Power and Paranoia in the Age of Fiber Optics. mit Press, 2008.
11. Deleuze, Gilles. "Postscript on the Societies of Control." October 59 (1992): 3–7.
12. Dubrofsky, Rachel E., and Shoshana Amielle Magnet. Feminist Surveillance Studies. Duke University Press, 2015.
13. Elsden, Chris, David Chatting, Abigail C. Durrant, Andrew Garbett, Bettina Nissen, John Vines, and David S. Kirk. "On Speculative Enactments." In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 5386–5399. ACM.
14. Evans, Dave. "The Internet of Things: How the next Evolution of the Internet Is Changing Everything." CISCO White Paper 1, no. 2011 (2011): 1–11.
15. Fiske, John. "Surveilling the City: Whiteness, the Black Man and Democratic Totalitarianism." Theory, Culture & Society 15, no. 2 (1998): 67–88.
16. Fraser, M. 2010. ''Facts, Ethics and Event.'' In Deleuzian Intersections in Science, Technology and Anthropology, edited by C. Bruun Jensen and K. Ro¨dje, 57–82. New York, NY: Berghahn Press.
17. Galloway, Alexander R. Protocol: How Control Exists after Decentralization. MIT press, 2004.
18. Gaver, William. "What Should We Expect from Research Through Design?" In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 937–946. CHI '12. New York, NY, USA: ACM, 2012.
19. Gaver, William. "Making Spaces: How Design Workbooks Work." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1551–1560. ACM, 2011.
20. Gaver, Bill, Tony Dunne, and Elena Pacenti. "Design: Cultural Probes." Interactions 6, no. 1 (1999): 21–29.
21. 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.
22. Gordon, Avery F. Ghostly Matters: Haunting and the Sociological Imagination. U of Minnesota Press, 2008.
23. Haggerty, Kevin D., and Richard V. Ericson. "The Surveillant Assemblage." The British Journal of Sociology 51, no. 4 (2000): 605–622.
24. "Hackers Use A Refrigerator To Attack Businesses - Business Insider.pdf." Accessed September 15, 2017. https://wecanfigurethisout.org/ENERGY/Lecture_notes/Smart_Grid_Supporting_materials/Hackers%20Use%20A%20Refrigerator%20To%20Attack%20Businesses%20-%20Business%20Insider.pdf.
25. Hanington, Bruce, and Bella Martin. Universal Methods of Design: 100 Ways to Research Complex Problems, Develop Innovative Ideas, and Design Effective Solutions. Rockport Publishers, 2012.
26. Harmon, Ellie, and Melissa Mazmanian. "Stories of the Smartphone in Everyday Discourse: Conflict, Tension & Instability." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1051–1060. ACM, 2013.
27. Hu, Tung-Hui. A Prehistory of the Cloud. MIT Press, 2015.

28. Hong, Jason I., and James A. Landay. "An Architecture for Privacy-Sensitive Ubiquitous Computing." In Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services, 177–189. ACM, 2004.
29. Irani, Lilly C., and M. Silberman. "Stories We Tell About Labor: Turkopticon and the Trouble with Design." In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 4573–4586. ACM, 2016.
30. Irani, Lilly C., and M. Silberman. "Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 611–620. ACM, 2013. http://dl.acm.org/citation.cfm?id=2470742.
31. Kaplan, Caren. "Precision Targets: GPS and the Militarization of US Consumer Identity." American Quarterly 58, no. 3 (2006): 693–714.
32. Kuntsman, Adi, and Rebecca Stein. Digital Militarism: Israel's Occupation in the Social Media Age. Stanford University Press, 2015.
33. Leshed, Gilly, and Phoebe Sengers. "I Lie to Myself That I Have Freedom in My Own Schedule: Productivity Tools and Experiences of Busyness." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 905–914. ACM, 2011.
34. 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.
35. Lindley, Joseph, and Paul Coulton. "Back to the Future: 10 Years of Design Fiction." In Proceedings of the 2015 British HCI Conference, 210–211. ACM
36. Monahan, Torin. "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance." Communication and Critical/Cultural Studies 12, no. 2 (2015): 159–178.
37. Monahan, Torin. "Counter-Surveillance as Political Intervention?" Social Semiotics 16, no. 4 (2006): 515–534.
38. Michael, Mike. "'What Are We Busy Doing?' Engaging the Idiot." Science, Technology, & Human Values 37, no. 5 (2012): 528–554.
39. Odom, William T., Abigail J. Sellen, Richard Banks, David S. Kirk, Tim Regan, Mark Selby, Jodi L. Forlizzi, and John Zimmerman. "Designing for Slowness, Anticipation and Re-Visitation: A Long Term Field Study of the Photobox." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 1961–1970. ACM, 2014.
40. 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. DIS '17. New York, NY, USA: ACM, 2017.
41. Pierce, James, and Carl DiSalvo. Network Anxieties Design Packets. In Proceedings of Research through Design Conference 2017.
42. Pierce, James. "Design Proposal for a Wireless Derouter: Speculatively Engaging Digitally Disconnected Space." In Proceedings of the 2016 ACM Conference on Designing Interactive Systems, 388–402. ACM, 2016.
43. Pierce, James, Phoebe Sengers, Tad Hirsch, Tom Jenkins, William Gaver, and Carl DiSalvo. "Expanding and Refining Design and Criticality in HCI." In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2083–2092. ACM, 2015.
44. Seigworth, Gregory J., and Melissa Gregg. "An Inventory of Shimmers." The Affect Theory Reader, 2010, 1–25.
45. Sengers, Phoebe. "What I Learned on Change Islands: Reflections on IT and Pace of Life." Interactions 18, no. 2 (2011): 40–48.
46. 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.
47. Stapper, Pieter and Elisa Giaccardi. "Research through Design." The Encyclopedia of Human-Computer Interaction, 2nd edition. The Interaction Design Foundation. Accessed January 8, 2018. https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/research-through-design.
48. Troshynski, Emily, Charlotte Lee, and Paul Dourish. "Accountabilities of Presence: Reframing Location-Based Systems." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 487–496. ACM, 2008.
49. Tufekci, Zeynep. "Why'Smart'Objects May Be a Dumb Idea." New York Times, 2015.
50. "Uber Is Being Slammed for Its 'surge Pricing' after the London Terror Attack." The Independent, June 4, 2017. http://www.independent.co.uk/news/uk/home-news/london-terror-attack-uber-criticised-surge-pricing-after-london-bridge-black-cab-a7772246.html
51. Uscinski, Joseph E., and Joseph M. Parent. American Conspiracy Theories. Oxford University Press, 2014.

52. "Silicon Valley's $400 Juicer May Be Feeling the Squeeze." Bloomberg.com, April 19, 2017. https://www.bloomberg.com/news/features/2017-04-19/silicon-valley-s-400-juicer-may-be-feeling-the-squeeze.

53. Wakkary, Ron, William Odom, Sabrina Hauser, Garnet Hertz, and Henry Lin. "Material Speculation: Actual Artifacts for Critical Inquiry." In Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives, 97–108. Aarhus University Press, 2015.

54. Weiser, Mark. "The Computer for the 21 St Century." Scientific American 265, no. 3 (1991): 94–105.

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

56. Wilson, Dean Jonathon, and Tanya Serisier. "Video Activism and the Ambiguities of Counter-Surveillance." Surveillance & Society 8, no. 2 (2010): 166–180.

57. Wolf, Tracee Vetting, Jennifer A. Rode, Jeremy Sussman, and Wendy A. Kellogg. "Dispelling Design as the Black Art of CHI." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 521–530. ACM, 2006.

58. 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. CHI '07. New York, NY, USA: ACM, 2007.