Geoforum 49 (2013) 279–288

Contents lists available at SciVerse ScienceDirect

Geoforum

journal homepage: www.elsevier.com/locate/geoforum

Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks

Torin Monahan [a,*], Jennifer T. Mokos [b]

[a] Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA
[b] Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

ARTICLE INFO

Article history:
Available online 7 March 2013

Keywords:
Surveillance
Crowdsourcing
Mobile phones
Pollution
Outsourcing

ABSTRACT

Mobile systems for detecting environmental threats may radically restructure spatial imaginaries as people learn to see and engage with heretofore largely hidden dimensions of urban spaces. While the design of such technological systems is contingent and currently open to varied outcomes, powerful security and industry players are asserting their influence to set overriding protocols that will ensure widespread ambient data collection, especially for security and commercial applications. This paper critically explores the emergent power geographies of surveillance revealed by one such system: the Department of Homeland Security's Cell-All project. This project, which has been under development at the U.S. Department of Homeland Security (DHS) since 2007, equips mobile phones with chemical-agent detectors and links them to security networks so that threats to urban populations can be automatically detected and rapidly mitigated. In order to assess the politics of crowdsourced sensing systems, first we map the core characteristics of the Cell-All development model: creating a participatory system, building public–private partnerships, and outsourcing responsibility for privacy protections. Second, we describe some alternative designs for mobile, participatory environmental sensing and reflect on their potentials for correcting power inequalities or achieving environmental justice. Finally, we conclude by discussing the implications of these various systems and the conditions that could alter their outcomes.

1. Introduction

The securitization of urban spaces is a dynamic political process that mutates according to constructions of threat, need, and possibility. In some instances fear of terrorist attacks has motivated the hardening of potential targets, such as monuments or buildings, with video surveillance networks or concrete sacrificial facades intended to block would-be bombers (Boddy, 2007; Coaffee, 2004; Fussey et al., 2011). In other cases, unmanned aerial vehicles are deployed over cities and borders to watch for illegal or suspicious activities and direct authorities to investigate (Finn and Wright, 2012; Graham, 2010; Wall and Monahan, 2011; Weber, 2011). Other articulations come in the form of informatized passage points, such as building entrances, community guard stations, or airports, where biometric identifiers and identity documents can be checked to ascertain whether one should be granted access (Adey, 2006; Klauser, 2010; Lianos and Douglas, 2000; Magnet, 2011; Thrift and French, 2002). Such systems often act in overlapping and reinforcing ways, connecting with larger assemblages of regulation and control. As geographers and surveillance studies scholars have argued, the modalities of security systems are inflected by an anticipatory rationality that seeks to identify and control risks in advance (Coaffee et al., 2009; Graham and Wood, 2003; Haggerty and Ericson, 2006; Klauser et al., 2008; Lyon, 2003). Rather than being objective or deterministic, however, every step in the process—from risk construction to system implementation to altered practice—betrays a complex politics whereby resources are allocated, populations sorted, and institutions reconfigured.

An important dimension of the securitization process is the creation of compelling narratives to justify the surveillance systems under consideration. This mythical dimension relies on what Mike Crang and Stephen Graham (2007) have called "technological fantasies" that position emergent technological systems as necessary—and effective—responses to dire threats. Some of the genres at work are entertainment media and news reporting; police or government educational campaigns; and industry- and government-produced videos, presentations, and reports that typically describe scenarios of mass destruction, followed by proposed technological fixes to prevent or manage such crises (Altheide, 2006; Barnard-Wills, 2012; Graham, 2010). As has been argued elsewhere, technological fantasies are not simply instrumental narrative devices to achieve desired ends; in addition to this, they actively shape larger security cultures and afford them influence,

* Corresponding author.
E-mail addresses: torin.monahan@unc.edu (T. Monahan), jennifer.mokos@vanderbilt.edu (J.T. Mokos).

0016-7185/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.geoforum.2013.02.001

such that alternative motivations for personal or institutional action become filtered through a security lens (Monahan, 2010b).

The technological fantasy that is the backdrop for this paper is one where mobile phones are equipped with chemical-agent detectors and linked to security networks so that threats to urban populations can be automatically detected and rapidly dealt with. This project, which has been under development at the U.S. Department of Homeland Security (DHS) since 2007, operates under the name "Cell-All." It draws upon an existing ecology of related sensor networks woven throughout the built environment in many cities, such as Chicago's "Operation Virtual Shield," which includes smart CCTV cameras and hidden chemical and biological agent sensors (Bulkeley, 2009; Murakami Wood, 2009a). The name Cell-All references the ubiquity of mobile phones and perhaps unintentionally signals the data exchange made possible by the public–private partnerships that are at the heart of this enterprise. The DHS Cell-All project is also designed to exploit mobile-phone saturation to enroll everyday users as passive data collectors whose devices communicate silently to the DHS system and its private industry partners. As with U.S. border-control and military efforts to enlist citizens as participants in crowdsourced surveillance (Koskela, 2010; Murakami Wood, 2009b), the success of Cell-All depends upon a mass of participating individuals scanning public spaces.

The ideological underpinning for the Cell-All project is one of neoliberal public–private partnerships, by which industry profits from privileged government contracts and access to data without accepting many financial or symbolic risks. A core component of this arrangement, as will be shown, is in the persuasion of everyday mobile phone users to act as data collectors and distributors. In this sense, to achieve initial success a certain type of participatory surveillance must be cultivated through discursive appeals to individuals—whether patriotic duty to avert mass-casualty disasters, personal interest to save oneself or one's loved ones from carbon monoxide poisoning, or individual desire to be a part of an innovative technological research project. Regardless of the nature of the appeal, the intended outcome is for the responsibilization of individuals to undertake what Mark Andrejevic has referred to as the "work of being watched," an eager involvement in data collection and restricted forms of interactivity that may give one pleasure while simultaneously serving the interests of institutions (Andrejevic, 2002, 2007).

While the Cell-All project may rely upon a technological fantasy, it is certainly not fictional. Prototypes have already been developed, major telecommunications companies have become partners, and mass-marketing strategies are being fine-tuned. Drawing upon insights from the field of science and technology studies, one could say that the "black box" of this technology is rapidly closing and its politics are solidifying; as a result, alternative, perhaps more democratic and empowering possibilities are being foreclosed (Akrich, 1992; Winner, 1986; Woodhouse et al., 2002). Once mobile phone manufacturers routinely include chemical and other sensors in their devices, users can be compelled or coerced to communicate environmental data as such sharing becomes normalized in technical protocol. There is precedent in place to require geolocational data sharing as an "always on" feature of mobile phones for purposes of public safety under the E911 initiative in the U.S. and similar requirements in other countries (Curry et al., 2004), so one can easily envision similar policies mandating the constant relay of environmental readings. This predictable development makes sense in part because of the widespread normalization of surveillance through commonplace media and organizational encounters. As David Murakami Wood and William Webster explain: "Interactions become structured around surveillance relationships and the new forms of social negotiation that emerge are no longer about what information one chooses to give but how that information is to be given (or taken)" (Murakami Wood and Webster, 2011: 157).

In keeping with the goals of this special issue, this paper will critically explore the emergent power geographies of surveillance revealed by DHS's Cell-All project. Environmental sensing with mobile devices represents, on one hand, the possibility for crafting new spatial imaginaries and modes of public engagement that bring about collective empowerment. On the other hand, technological systems must be situated within their current political and ideological contexts, which in the case of Cell-All signifies a tightly constrained trajectory for technology development that promises coerced participation and asymmetrical relationships of visibility. First, we will provide an overview of our methods and sources. Second, we will draw upon DHS documents and presentations to analyze the Cell-All project, paying particular attention to the core characteristics of its development model: creating a participatory system, building public–private partnerships, and outsourcing responsibility for privacy protections. Third, we will describe some alternative designs for mobile, participatory environmental sensing and reflect on their potentials for correcting power inequalities or achieving environmental justice. Finally, we will conclude by discussing the implications of these various systems and the conditions that could alter their outcomes.

2. Methods and sources

The primary case study analyzed here—that of the Cell-All system—is based on a review of official and public documents, including press releases, media reports, DHS documents and training materials, and commercial partner marketing products and websites. We conducted a LexisNexis news search to identify news, media, and publicly available materials referencing Cell-All. All articles returned by the search were examined for relevance, and those not directly discussing the Cell-All program were discarded, with 31 documents remaining. These relevant documents were read and coded to identify initial thematic concepts in accordance with grounded theory approaches to data analysis (Charmaz, 2006).

In response to initial thematic coding, additional targeted data collection was focused on DHS and commercial partner documents and websites in order to identify the current development status, the operation and functionality of the system, and marketing strategies. This secondary investigation included a thorough search for pertinent documents on DHS's website, as well as searches on commercial partner websites, to locate original agency and company texts. A 2-hour video webcast of the DHS's live demonstration and training of the Cell-All project held at the Los Angeles Fire Department's Frank Hotchkin Memorial Training Center on September 28, 2011 (U.S. Department of Homeland Security, 2011a) was also transcribed and coded. Analysis of primary DHS and commercial partner documents yielded key information on the design of the Cell-All system, from the environmental sensors to the broader support and data communication infrastructures developed to store, analyze, and send alerts.

Many of the media and news articles identified were printed in security trade publications, such as Aviation Today's *Air Safety Week* and the *Terror Response Technology Report* (*TR2*), and they were often published in response to press releases from DHS or other Cell-All partners, such as NASA's Ames Research Center. This dynamic tended to produce clusters of articles with similar headlines and content that often closely reproduced the phrasing and content of the agency press releases. Similarly, the few articles that did appear in the mainstream media seemed to echo statements made in press releases with little or no analysis. This relationship between press releases and media reports suggests that there

may be a disproportionate ability afforded to DHS and commercial entities to shape public understanding and uptake of these technological systems.

3. Exploring the DHS Cell-All project

3.1. Project background and development

Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones.

The Homeland Security Advanced Research Projects Agency (HSARPA) of the DHS Science and Technology (S&T) Directorate refers to the sensors as "a new class of chemical detectors" that are smaller, less expensive, and *in situ* compared to the fairly large, static, and relatively expensive sensors used at existing monitoring stations (U.S. Department of Homeland Security, 2011a). By drawing upon mobile phone saturation, the Cell-All program aims to establish a flexible and dynamic sensor system, with citizens functioning as roving information nodes. As Stephen Dennis, the technical director of HSARPA, states, "Generally people have their smartphone with them. It's representing [through sensor readings] the space that they reside in" (Dennis, 2011).

For the program's initial phase in 2007, DHS released a call for proposals inviting the private sector to develop a proof of concept for the "Cell-All Ubiquitous Biological and Chemical Sensing" project (U.S. Department of Homeland Security, 2007). The goals at this point were to design a range of chemical sensors and refine the GPS functionality of phones to achieve accurate transmission of location data. According to DHS, the first year and a half focused on the question "Could we miniaturize chemical sensors and make them actually fit a cell phone profile?" (Dennis, 2011). Thus, researchers focused on understanding the needs of the equipment, in terms of power and physical profiles, and determining whether the sensors could work within the "ecosystem of the phone." HSARPA conducted a national search for ideas that was intended to leverage existing technological expertise in the public and private sectors, which led to the creation of six workable first-generation prototypes, including a "form factor phone" developed by Qualcomm and a chemical nanosensor device developed by NASA (U.S. Department of Homeland Security, 2011a).

The second phase of Cell-All began in 2010 with the goals of creating dozens of competing viable devices and refining the network capabilities of the system (U.S. Department of Homeland Security, 2011a). At this stage, DHS also sought to standardize the data-reporting protocols so that data from different devices could be received and processed by a centralized network operations center. Research contracts were awarded by DHS through HSARPA and the Small Business Innovation Research Portfolio, with some of the primary recipients being Qualcomm, Synkera Technologies, and NASA (U.S. Department of Homeland Security, 2011b). In addition, DHS S&T secured Cooperative Research and Development Agreements with four primary cell phone manufacturers—Qualcomm, LG, Apple, and Samsung—with the objective of accelerating the "commercialization of technology developed for government purposes" (U.S. Department of Homeland Security, 2010).

During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available. At a September 2011 live test and demonstration of second-generation prototypes at the Los Angeles Fire Department's Frank Hotchkin Memorial Training Center, Synkera's prototype was already on the market and NASA's sensor was awaiting clearance for public release. DHS presentations at this event conveyed that next generation, sensor-embedded phones would roll out gradually over the next few years and, as with cameras in phones, would soon become standard (U.S. Department of Homeland Security, 2011a).

3.2. Cultivating participation through a personal alerting system

A 2011 report by Fox News begins with the following scenario: "A silent killer threatens a family with a baby in a hotel room. Fortunately, their smartphone wises up, senses the threat and notifies the authorities—and the local fire department charges in to the rescue, saving the day" (Barrie, 2011). The silent killer in this story is that of carbon monoxide, which causes thousands of poisonings and hundreds of deaths each year (King and Bailey, 2007), and the smartphone is equipped with gas sensors and linked directly to DHS's Cell-All system, allowing for automatic communication with first responders. The fictional story continues by escalating the life-saving potential of the systems to mass casualty terrorist attacks:

> Ultimately, Cell-All could be American's secret weapon against public threats at football stadiums or sarin gas-style attacks like the one that killed 13 people in Tokyo's subway system in 1995. Experts are always working hard to find ways to reduce the risk to Americans at large events that could be attractive targets to terrorists. (Barrie, 2011)

As with other surveillance systems deployed under the rubric of counterterrorism, the accompanying narrative implies technological infallibility and nurtures public support through a process of simplification that strips away politics and social difference (Monahan, 2010b). What is especially interesting about this media thread, though, is that it emphasizes personal, commonplace threats (carbon monoxide poisoning of families) over large-scale terrorist attacks. This may indicate a larger shift in security discourses, but it also suggests an intentional crafting of message, on the part of DHS and its partners, to encourage participation of and support by the growing population of smartphone users in the U.S.

Therefore, during the second phase of development outlined above, DHS shifted its marketing strategy to stress the personal protection aspect of the project as an approach intended to persuade consumers to buy the associated products (U.S. Department of Homeland Security, 2011a). So, whereas in 2010 media articles and a DHS press release focused on the homeland security potential of the sensors to detect biological and chemical terrorist agents, for example by calling it a "handheld weapon of mass destruction detector" (U.S. Department of Homeland Security, 2010), in 2011 the technology was instead described as a "personal environmental threat detector system" (U.S. Department of Homeland Security, 2011c: 37) and an "environmental surveillance system" (U.S. Department of Homeland Security, 2011b: 2). By the time of the 2011 Cell-All product demonstration, presenters

concentrated almost exclusively on threats posed by commonplace gas or chemical exposure, such as carbon monoxide in the home or toluene in nail salons. Furthermore, while a range of sensors are available to detect chemicals, such as chlorine, carbon monoxide sensors were the ones first linked to the Cell-All platform and made available for purchase (Li, 2011).

Unlike most state-sponsored security programs, which are implemented without full public knowledge or direct approval, the public–private partnership model adopted by Cell-All requires public buy-in, at least initially. This necessitates the adoption of a market lens to evaluate the need for and potential success of this public safety program. As DHS's Stephen Dennis explained, "We didn't just do the science work here; we actually did look at the market" (Dennis, 2011). With Qualcomm's help, DHS assessed commercial viability through market research, asking what conditions would need to be met for the public to both accept and pay for the system. Based on this market research, DHS concluded:

> What we learned is that the personal protection application will sell the device. People will actually turn in their [current] phone, get a new phone, if it provides them with a magnitude of personal protection, especially for families, people with aging parents, people with young children. (Dennis, 2011)

In order to convince people that the system would assist with personal protection, DHS settled on carbon monoxide poisoning as a much more likely and avoidable threat than terrorism. Mainstream media outlets like Fox News could provide sensationalistic sales-pitch stories about the "silent killer" of families with babies, while DHS could craft an argument drawing upon sober statistics and the expertise of first responders:

> When we asked our nation's first responders to name the deadliest gas for us, in terms of what the American population faces as a threat, carbon monoxide was it…it actually establishes a basis for commercial manifestation of what we've done here. (Dennis, 2011)

Thus, by the time of DHS's live demonstration of their system in 2011, the entire framing had shifted to "infiltrations" of carbon monoxide as an invisible and unpredictable danger to Americans:

> Today's test is going to focus on a common poisonous gas that is responsible for more than 2,000 deaths in the United States every year. As a matter of fact, just yesterday there were 43 people injured in an incident in Washington D.C. where carbon monoxide gas infiltrated into a building. (Verrico, 2011)

The marketing efforts that follow these threat constructions focus almost exclusively on the individual, positioning the product as a personal alerting system.

As a personal sensing and alerting system, Cell-All promises to protect a diverse and inclusive range of individuals, from "a grandmother taking a siesta [to] a teenager hiking through the woods…" (U.S. Department of Homeland Security, 2010). When set to personal safety mode, an auditory alarm will sound directly on the phone when the sensor detects an abnormal chemical level, and the app can also be configured to send a text message to specific emergency contacts designated by the user. While the sensing data ostensibly remain within the sphere of users and their designated contacts, in order to take advantage of these data for other purposes, such as ensuring public safety, the program includes plans for automatically reporting personal alerts to an independent monitoring service (U.S. Department of Homeland Security, 2011a). By expanding the data network in this way, DHS hopes to harness the collective potential of mobile phones as public environmental sensing devices for "crowdsourcing human safety" (U.S. Department of Homeland Security, 2010).

As a starting point, users will be given the choice of opting-in to wider sharing of their sensing data:

> We're asking the public if they would like to opt-in to a network, an anonymous network, an anonymous report, of what is it that their phone has seen to an operations center that can then understand what it is that that sensor and the collection of sensors around them actually means in terms of response. (Dennis, 2011)

One can note in this articulation the incipient unfolding of an argument for access to—and control of—data by organizations that can "understand" what an alert "actually means." Beyond the personal alert functionality, the larger goals are to aggregate data from multiple cell phones located within crowded public areas, such as sports arenas, subway stations, or office buildings. Then in addition to sending an individual alert, each phone on the network could send abnormalities detected by the sensors directly to a centralized network operations center (NOC). The idea is that the NOC will be equipped to analyze the reports within the context of each other (as well as other available data) and the aggregation of sensors in crowded public places will minimize false positives. One phone reporting an abnormal chemical level could be an error; a hundred phones reporting the same levels would be more likely to indicate a situation in need of intervention. When the NOC identifies that a threat is likely, it could then contact local agencies and first responders.

In order for Cell-All to succeed as it moves along a path from personal protection to centralized data collection, it must both compel and automate participation in data-sharing schemes. DHS rationalizes this as placing trust in objective technological systems instead of supposedly unreliable and error-prone individuals:

> Currently, if a person suspects that something is amiss, he *might* dial 9-1-1, though behavioral science tells us that it's easier to do nothing. If he does do something, it may be at a risk to his own life…the caller may be frantic and difficult to understand, diminishing the quality of information…An even worse scenario: the person may not even be aware of the danger, like the South Carolina woman who last year drove into a colorless, odorless, and poisonous ammonia cloud. (U.S. Department of Homeland Security, 2010)

In this example, it is not obvious how a cell-phone sensor would have helped, and according to other sources the woman, who died, left her vehicle because she was aware of the gas (Associated Press, 2009). Still, the example hints at scenarios where an automated Cell-All system might save lives, such as if multiple sensor readings prompted a rapid evacuation and quarantine of contaminated areas. Automated data sharing, a fully functional infrastructure, and tight coordination with first responders would be necessary components for this to be effective.

In the marketing of Cell-All, personal protection serves as the initial hook, allowing for data sharing to be expanded gradually. First this will take the form of opting-in to sharing data with a network operations center, with assurances that personal identifiers will be scrubbed from the data. Next, if precedent holds, wider data sharing will occur and participation will become compulsory. A neoliberal ideological context shapes the Cell-All project as a whole, as we will discuss further in the next section, but it also motivates government agencies to formulate problems in such a way that market-based solutions become logical responses to them.[1] Therefore, rather than tackle the health dangers posed by

[1] The neoliberal context signifies, in part, a market rationality of privatization of public goods and institutions, deregulation of industry, and responsibilization of individuals for the provision of human security and social reproduction (Monahan, 2010a, 2010b).

cumulative exposure to contaminants or impose tighter regulations upon chemical and other polluting industries, DHS focuses on individual responsibility for mitigating threats as a gateway to supposed wider public protection from catastrophic events. Just as individuals are being charged with maintaining the integrity of their digital identities online (Whitson and Haggerty, 2008), Cell-All hints at new articulations of responsibility where individuals will be enlisted symbolically as data collectors of environmental threats, fulfilling their biochemical duty to keep themselves and their families uncontaminated.

Enrolling members of the public could be seen as an entrepreneurial move on the part of DHS to exploit existing public resources, in the form of people with smartphones, to meet its narrowly defined public-safety objectives; as a Qualcomm representative argued: "Let's take advantage of the 300 million cell phones that are out there today. They're always with us" (Hoffman, 2011). Widespread participation is needed, with members of the public serving as passive data-collection nodes, but the program's goals do not include promoting environmental expertise among everyday users. The model for achieving such protection depends on centralized data collection so that experts and authorities can act to minimize or respond to threats. Although public protection may never actually be achieved by this system, it nonetheless advances public–private partnerships that further normalize the collection of sensitive, personal data for purposes of profit and control.

3.3. Forging public–private partnerships

The Cell-All program is funded and managed by HSARPA, whose mission is to facilitate the rapid development *and* deployment of new security technologies, mainly through partnerships and contracts with the private sector (U.S. Department of Homeland Security, 2011a). As DHS representatives explain it:

> The most important component of all is delivering the technology into the hands of those who need it so that we're not one of those government R&D labs that's happy to throw something over the wall or end it with a paper. We're actually trying to take this technology all the way to the end. (Dennis, 2011)

HSARPA accelerates this process through direct commercial partnerships, where it funds researchers from both the public and the private sector to develop products that can then be brought to market, even if the only buyers are government agencies.

The resulting neoliberal arrangements mirror those in other industries—such as pharmaceutical research and development, where in the U.S. the vast majority of research is paid for by public funds and conducted in university labs, after which time pharmaceutical companies acquire those research findings to develop profitable drugs without distributing revenue back to the public sector (Angell, 2004; Fisher, 2009). More than simply being probusiness, such arrangements seek to privatize government functions through partnerships and reconstruct the public good as that which benefits industry. Public subsidization of private companies, whether in the domains of homeland security or pharmaceuticals, is rationalized through discourses of efficiency. In the example of Cell-All, DHS justifies such partnerships by saying:

> We believe that technology transfer directly to the commercial [sector] is an efficient way to go. We know that there are a number of commercial opportunities that have been provided to our sensor manufacturers and to the folks who are involved in this program, so we're looking forward to taking advantage of those [opportunities] directly. (Dennis, 2011)

Therefore, although Cell-All is managed and funded by HSARPA, the technologies and infrastructures are being developed by third party contractors who received funding from DHS for those purposes and who can then profit further from the sale of any resulting systems or services (U.S. Department of Homeland Security, 2011a,c). Currently, the primary contractors working on the project are Synkera Technologies, Qualcomm, NC4, and NASA's Ames Research Center, which is the only public agency receiving a contract.

Each of the organizational entities involved in the project are working on separate system components that will be integrated as the project progresses. The exception is the NASA research center, which appears to be on a parallel development track to the industry partner Synkera, although it is not clear how much intellectual property is being transferred from NASA to Synkera or the other companies. In order for the Cell-All public safety sensing and alerting system to be complete, four links must be forged and joined together: the sensor and computing hardware, the sensing application for mobile phones, a centralized server and network operations center, and the end consumer, whether individuals, emergency operations centers, first responders, government agencies, or private companies. Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones—that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).

Qualcomm's role has been to develop a smartphone app and the associated network software for processing data. Smartphone users can download the app from Google Play and, eventually, from Apple's iTunes store, so Cell-All will be operational on all phones using either Google's Android or Apple's iPhone operating systems. When the application is installed it will ask the user for permission to share sensor readings and location information over the network; then, whenever abnormal chemical levels are detected, the phone will send those data to a network gateway. According to Doug Hoffman, program manager at Qualcomm, the gateway will authenticate the sensor and phone to determine whether they are authorized to be on the network, scrub personal information from the data, assign a temporary identification number to the phone, and then send data to the network operations center (NOC) (Hoffman, 2011).

The NOC acts as a data-clustering algorithm that combines and analyzes data from multiple phones in terms of geographical location, time, and chemical level in order to determine whether there is an abnormal public safety event. The NOC servers also have the ability to communicate directly with phones to change the frequency with which the phone is reporting data. For example, if there is a major risk-event involving many cell phones, the NOC can request less frequent reporting so that the network is not overloaded.

If the NOC algorithms determine that there is a potentially dangerous situation, an alert is transmitted to a "risk center" run by the California-based security company NC4. Established in 2001 after the attacks of 9/11, NC4 specializes in "situational readiness," which it aspires to obtain by bridging "the communication gap in a post-9/11 environment between the public sector and the private sector" (Needs, 2011). NC4's customers include both private and public sector organizations oriented toward security, risk management, and emergency response. The company operates two "risk centers," one on each U.S. coast, where analysts receive and vet data from NOCs and other sources before communicating threats to others or assisting with responses. Essentially, NC4 risk centers function as private-sector "fusion centers," much like DHS data fusion centers that are intended to identify threats in advance, assist

law-enforcement investigations, and coordinate responses (Monahan and Palmer, 2009).

According to Chris Needs, product and content manager at NC4, the risk centers perform a "human-in-the-loop" function of looking at raw data from the sensors, comparing them with data from other sources, and translating them into alerts that can be sent, for a fee, to end users, whether first responders, government agencies, individual consumers, or private-sector commercial entities.[2] For example, during the Cell-All live demonstration in 2011, alerts were sent to the Los Angeles emergency operations center, which could have then dispatched first responders or managed the threat were it real. The service provided by NC4's risk centers is marketed as generating "value-added" alerts that can include maps of locations with spikes in sensor readings, "so if you're not familiar with the area you can see how far is this incident from my sensitive assets" (Needs, 2011).

There is certainly a great deal of coordination required by DHS to bring the program components together for Cell-All to even approach operational status. From the start, though, the program has fostered public–private partnerships under the assumption that government agencies are too slow or lack the expertise to develop such a system on their own. This position is neatly articulated by HSARPA:

> The acceleration of integrated environmental sensing and the utilization of mobile computing platforms for homeland security establishes a leading edge capability instead of a traditional trailing edge capability that government sometimes has, taking advantage of the latest in new chemical sensor innovation. Delivering these capabilities to the extended homeland security enterprise as a commercial capability makes government technology transfer easier and far more efficient than trying to nurse it along inside of government, so I'm very excited that we have commercial opportunities to take advantage of the technology that's been created here. (Dennis, 2011)

NC4's CEO and president Jim Montagnino puts it a bit more bluntly, actually implying that government bureaucracies invite security threats: "Bureaucratic red tape impedes critical information sharing across organizational boundaries, which leaves the door open to national security threats" (Montagnino, 2012).

Framed in this way, the expedient solution is neither to concentrate on problems that government is equipped to solve, such as passing and enforcing environmental regulations, nor is it to streamline government agencies, although that option certainly exists as an imperative within neoliberal cultures. Rather, the task is seen as finding ways to entice industry to "partner" with government agencies, mainly by ensuring profitability for private companies (Monahan, 2010b). This orientation is evinced by Cell-All's early-stage market research, paid for by HSARPA and administered by Qualcomm. After finding a viable market, industry partners were further persuaded by government contracts to develop systems and services and by the high probability of sustained profits from a range of customers after product development. Clearly, having privileged access to consumer data, even in de-identified, aggregate form, would be of great interest to partnering companies.

3.4. Outsourcing privacy protections

During the research and development phase of projects like Cell-All, privacy risks are the responsibility of DHS's S&T Directorate, which conducts privacy impact assessments (PIAs) for laboratory- and field-testing. However, once S&T raises a technology to operational status, the responsibility for evaluating emerging privacy risks typically falls upon the privacy offices of the respective entities involved, such as Immigration and Customs Enforcement, the Transportation Security Administration, the Coast Guard, or others (U.S. Department of Homeland Security, 2011c). This separation between research and operational responsibilities for privacy protection may have particular implications for Cell-All because the final deployment of the technology will also have a commercial component. When government entities constitute the end-user community, the DHS Privacy Officer may require that privacy impact assessments be incorporated into the implementation process (Clarke, 2009); however, the private companies that will be managing core components of Cell-All are under no such obligations.

While one might expect that the early-stage PIA conducted by DHS would nonetheless anticipate real-world operational deployments of Cell-All, this is not the case. Instead the focus is on ensuring privacy protections for the development and pilot-testing phases (U.S. Department of Homeland Security, 2011b). To accomplish this, DHS adopted what is akin to institutional review board (IRB) review for human subjects research, including obtaining informed consent from participants. Thus, for a 2011 personal safety demonstration of Cell-All at the Los Angeles Fire Department test facilities, first responders participating in the demonstration consented to the transfer of geolocational data over the network but not personally identifiable information, such as mobile phone numbers (U.S. Department of Homeland Security, 2011a). As is standard with informed consent for research, "users participating in the test [were told that they] may turn off their cell phone and stop participating in this test at any time" (U.S. Department of Homeland Security, 2011c: 38). After testing is complete, however, the system "will be transitioned to the private sector and marketed by commercial vendors" (U.S. Department of Homeland Security, 2011c: 39), such that responsibility for privacy protections will be handed-off to those companies.

The model of outsourcing privacy protections to private companies engenders some interesting discursive moves on the part of DHS representatives, who say things like: "While Cell All was designed with privacy protections in mind, the end user community must continue to consider privacy when deploying the system for operational use" (U.S. Department of Homeland Security, 2011b: 7). After deployment, those managing the system will determine whether they want to collect cell phone numbers, users' locations and movement, or all chemical readings, rather than only ones deemed "significant." This position is made clear by a DHS privacy impact assessment that states:

> Decisions regarding the capture and transmission of additional information (e.g., phone numbers, names of cell phone owner) will also be decided by the end user community, with input from the first responder community, and public health organizations, among others. (U.S. Department of Homeland Security, 2011b: 6)

DHS dismisses any future privacy concerns by implying that individual users will always be able to opt-out of the system if they feel uncomfortable: "Privacy is as important as technology... After all, for Cell-All to succeed, people must be comfortable enough to turn it on in the first place" (U.S. Department of Homeland Security, 2010). For DHS, operational risks are narrowly defined in terms of market failure, not potential problematic uses of personal data, lack of transparency about data being collected and shared, or the coercive effect of technological protocols that may resist easy rejection.

As has been demonstrated with other dimensions of surveillance societies, private companies have an interest in amassing

[2] The NC4 analysts continually monitor multiple government and media information streams, including social media.

as much personal data as possible in order to profit, whether by selling convenient products and services to users, providing data for a fee to government agencies, or minimizing risk more generally (Andrejevic, 2007; Lyon, 2001; O'Harrow, 2005). Without specific prohibitions against the collection and use of personal data, projects like Cell-All possess a strong valence toward applications that exceed the original scope of the project. The data produced from the system can also be funneled back to government agencies, just like DHS fusion centers pay to tap the repositories of private data aggregators to assist with investigations, even if such data would be illegal for fusion centers to collect on their own (Monahan and Palmer, 2009). In such situations, the systems can effectively evade public accountability because private companies, who maintain the databases, are shielded from open-records requests.

Privacy threats extend beyond the coercive collection and storage of personal information. Control over who has access to such information is also tenuous, as can be seen, for example, with the numerous cases of hundreds of thousands of electronic records of personal information being hacked, lost, or stolen—from private companies and government agencies alike (Gilliom and Monahan, 2013). Furthermore, even if accessed in aggregate form, data mining and big data analytics can produce startlingly accurate profiles, which could be used to further sort, discriminate against, or commercially target users (Andrejevic, 2011). Data analytics of commercial systems have also revealed the ease with which individual users can be reidentified, even when anonymity has been ensured (Gilliom and Monahan, 2013). Thus, Cell-All and similar systems further the process by which individuals become sensing nodes themselves, communicating valuable data to private companies, government authorities, and peers.

With Cell-All, there is also strong potential for mission creep because of organizational arrangements that make robust privacy protection voluntary and mobile technologies that afford the collection of highly granular data. As Katie Shilton has observed, "At the extreme, mobile phones could become the most widespread embedded surveillance tools in history" (Shilton, 2009: 48). When coupled with environmental sensors, the capacity of mobile phones to identify individuals and track their movements could lead to many kinds of social control and discrimination well beyond the disclosure of personal information. For instance, insurance companies could use such data to cancel an individual's medical coverage or increase premiums because one is routinely exposed to high levels of air pollution because of where he or she lives, works, or commutes. This is not that far fetched as there are existing corollaries with companies charging higher rates for property insurance when people live in high-crime areas, or with companies offering "lifestyle discounts" for people who can prove that they exercise regularly and eat healthy foods (Gilliom and Monahan, 2013). Other scenarios could include companies using sensor data from individuals' phones to make decisions about whom to hire or which employees to discipline; just like organizations currently can demand drug testing, sensor-embedded phones could reveal who is exposed to marijuana or tobacco smoke and therefore who might be deemed to be a risk to the company. The same might hold true for landlords requesting sensor data as a condition for considering tenants' applications, just as many landlords presently require credit checks when considering applications (Neighborhood Link, 2010). This list of examples could easily be expanded, but the point is that based on precedent such systems will lend themselves to coerced participation and sorting of populations based on perceived risk levels, so these outcomes should be anticipated in advance of system deployment.

4. Toward empowering participatory sensing

Cell-All serves as an influential case study, particularly because the program shapes technological designs and organizational models that will guide future endeavors in the area of mobile environmental sensing. It advances a dominant paradigm of surveillance predicated upon asymmetrical relations of visibility and control, on one hand, and industry profits, on the other. Additionally, as a case study, Cell-All is emblematic of wider trends in the development of restrictive spatial protocols for locational tracking and sensing. As socially constructed systems, though, such spatial and technological protocols need not be so restrictive, extractive, or controlling. A variety of alternative, more open and participatory designs are circulating, even as DHS and its industry partners are moving toward technological closure on mobile sensing systems.

Several scholars have been actively involved in theorizing such alternative surveillance trajectories, often in conversation with artists, engineers, and activists. For instance, David Murakami Wood has described the possibility of shared surveillance protocols that might build upon the inclusive ideals of universal design and open source movements to enrich people's lives and produce relationships of sociality (Murakami Wood, 2007). Katie Shilton, working through a number of persuasive case studies, refers to participatory sensing as an activity that "is meant to enable (and encourage) anyone to gather and investigate previously invisible data. It tries to avoid surveillance or coercive sensing by emphasizing individuals' participation in the sensing process" (Shilton, 2009: 50). Dana Cuff, Mark Hansen, Jerry Kang argue for embedded-network-sensing applications that advance social empowerment through the creation of a "data commons" that functions as "a data repository generated through decentralized collection, shared freely, and amenable to distributed sense-making not only for the pursuit of science but also advocacy, art, play, and politics" (Cuff et al., 2008: 29).

Many of the projects being developed by UCLA's Center for Embedded Networked Sensing (CENS) attempt to catalyze empowering participatory sensing. For example, the Personal Environmental Impact Report (PEIR) project encourages individuals to use their mobile phones as self-surveillance devices to track their daily exposure to air pollution and calculate their own carbon footprints (Shilton, 2009, 2012). By reading locational data against air-quality alerts and maps, the system determines the amount of pollution one is exposed to over a given time period. Also, by drawing upon the GPS and accelerometer sensors in most mobile phones, PEIR can surmise what mode of transportation one uses for commutes and estimate one's carbon footprint based on those data. The overall aim is clearly one of cultivating public awareness of pollution problems and motivating individuals to change their own behavior to minimize both exposure and contributions to air pollution. Beyond this, CENS seeks to push participatory sensing toward democratic and environmental justice outcomes, encouraging mobile phone users to document egregious pollution conditions, share those data with others, and mobilize findings—in consultation with scientific experts—to influence policymakers (Center for Embedded Networked Sensing, 2008). Although the vision does problematically imply that one could uncover indisputable truths that would necessarily lead to progressive policy changes, the power of this model of participatory sensing is in its semi-open protocol that foments new spatial imaginaries about pollution in urban environments and invites participants to use data for their own ends, whether for changing individual behaviors or organizing for social change.

Another provocative example is the Safecast system, which originated as a collective of individuals using mobile phones and

Geiger counters to map radiation levels in Japan during the nuclear crises precipitated by an earthquake and tsunami in 2011. During this period, many people purchased radiation detectors and shared "readings" through websites and social media as a mechanism by which to achieve collective knowledge about dangers when official information was seen as being insufficient or untrustworthy (Safecast, 2012). The Safecast network, which received some institutional support from the MIT Media Lab, embodied a hacker ethos of constructing do-it-yourself sensing technologies and openly sharing information to ensure public safety and achieve political aims (PBS NewsHour, 2011). In many respects, Safecast operated through shared protocols to actualize a robust data commons, showing the empowering potential of participatory surveillance. At the same time, the practices of this network may signal an almost complete decline of trust in public institutions, such that the primary purposes may be ensuring self-protection through disaster preparedness and response, not necessarily dismantling risky infrastructures or challenging government truth claims about safety.

The project known as Crowd (Soft) Control offers another foray into empowering possibilities for participatory sensing. Based out of Northwestern University's AquaLab, researchers are designing mobile-phone applications to collect visual and sound data that are currently absent in databases because they exist at sites that are less frequently traversed by mobile phone users (Rula and Bustamante, 2012). For instance, urban sound maps that document sound-pollution hotspots may be skewed because they are populated primarily with data along main travel corridors, leaving less traveled routes underrepresented. Similarly, while personal and public image databases are replete with pictures of the front of buildings, there is a dearth of photographs of the side or rear of buildings, where exhaust fumes may be entering through air intake vents. In both of these situations, voids are left in the empirical record such that environmental problems may be unrecorded and therefore invisible within existing systems, making the likelihood of remediation slim. Crowd (Soft) Control seeks to build upon user familiarity with existing smartphone platforms, such as FourSquare or Facebook Places, to incentivize, through virtual rewards, the collection of missing visual and sound data. For instance, AquaLab researchers have devised a prototype for a game called "Ghost Hunter," wherein players must use their mobile phones to take photographs of supposed ghosts, who happen to be in locations where images are currently missing in existing databases (Rula and Bustamante, 2012). The intention of the researchers is to collect data that could assist with planning for urban sustainability, while drawing attention to environmental problems. User involvement is highly structured and constrained, so this would not necessarily constitute a democratic or truly participatory sensing system, but it does point to the possibility of progressive outcomes emerging from such projects.

Each of these alternative participatory sensing systems, as well as others like them (e.g., Chang, 2012; Monahan, 2010a; Ottinger, 2010; The Impact Project, 2012), offers a strong counterpoint to the controlling tone of security projects like Cell-All. Rather than rely on constructions of threats that invite restrictions of rights, neoliberal outsourcing, and the hardening of urban spaces, such alternatives operate in a register of "cosmopolitan security," which, as Stephen Graham has elaborated, is a mode of security that seeks to "address the real risks and threats that humankind faces in a rapidly urbanizing world prone to resource exhaustion, spiraling food, energy and water insecurity, biodiversity collapse, hyper-automobilisation, financial crises, and global warming..." (Graham, 2012: 326). That said, participatory sensing applications oriented toward cosmopolitan security still exist within states of extreme social inequality, so rather than being empowering in any universal way, they may instead highlight conditions of unequal exposure and invite conversations about persistent environmental racism and injustice (Monahan and Mokos, 2010). As with other forms of interactive surveillance, such systems also run the risk of being captured by commercial or security interests such that the data could be used for purposes that were not initially intended (Ellerbrok, 2011); thus, a certain amount of vigilance will be necessary to keep protocols open and directed toward social justice ends.

5. Conclusion

Crowdsourced sensing systems may drastically restructure spatial imaginaries as people learn to see and engage with heretofore largely hidden dimensions of urban spaces. While the design of these technological systems is contingent and currently open to varied outcomes, powerful security and industry players are asserting their influence to set overriding protocols that will ensure widespread ambient data collection, especially for security and commercial applications. In order to assess the politics of these emerging systems, this paper has mapped some of the institutional arrangements guiding technological development and analyzed the logics behind design decisions.

With DHS's Cell-All project, the vision for participation is one where members of the public act as passive data collectors for an almost completely closed system, where participants do not have access to data or environmental alerts beyond the individual level and where there are no opportunities for defining outcomes. The public, in this model, will be enticed or coerced to engage in the labor of being watched. This may happen through promises of protection from gas or chemical poisoning, through patriotic goals of averting mass casualties from terrorist attacks, or simply through invisible protocols that opt users in to data collection and sharing. At the same time, information systems are always embodied (Blanchette, 2012; Kitchin and Dodge, 2011), so as this version of participatory sensing grows, spatial protocols may emerge to sort and direct flows of individuals, perhaps giving priority access at security checkpoints or commercial venues to people voluntarily participating in the system—or singling out non-participants for added scrutiny or exclusion.

The Cell-All system also seeks to produce innovative organizational arrangements that advance research and development through public–private partnerships. DHS programs like Cell-All identify a narrow set of statistically unlikely scenarios, such as chemical attacks of public places or carbon monoxide poisoning, then frame problems in such a way that private-sector solutions are seen as the most reasonable and expedient. Viability for commercial success is measured through market research, and financial risks to participating companies are offset through DHS grants and assurances of a guaranteed market of government agencies and first responders upon project deployment. The program will produce data, which are viewed as being inherently positive. Industry partners stand to profit as well from vast repositories of personal data collected from millions of mobile phones, even if the uses of such sensor data are not yet defined.

Finally, by outsourcing privacy protections to companies and agencies implementing the systems, DHS both sidesteps responsibility for ensuring adequate protection of personal data and opens the field for industry partners to discover profitable uses for data. Privacy impact assessments, which may be required of security systems implemented by government agencies, are conducted only for the relatively innocuous development and testing phases of the project. In actual use, companies can collect data freely as long as they receive consent from users, such as in the form of license agreements that people routinely accept without reading (Böhme and Köpsell, 2010). The mission creep potentials of such surveillance systems are high. More than simply being a threat to privacy,

sensor data could lead to discrimination against individuals or groups who are perceived as living in risky environments or possessing risky lifestyles; precedents are already in place for such institutionalized forms of discrimination based on credit checks, drug tests, or health history, so sensor data from phones—were they readily available—could easily contribute to such practices.

Alternative participatory sensing systems offer templates for how environmental data could be collected in ways that are more democratic, encouraging of the development of user expertise, and dedicated to social and environmental justice. In short, the potential is there to harness such surveillance systems in the pursuit of cosmopolitan security and social equality (Graham, 2012). Because environmental threats are not distributed evenly, in order to achieve the progressive goals of their designers, such alternative systems must foster collective understandings of and responsibility for toxic exposure so that mitigation of risk will not be further individualized without altering the systems producing threats. If encoded in sociotechnical systems and practices, the cultivation of shared risk-topographies of environmental threats could serve as a powerful corrective to Cell-All's emphasis on individual responsibility, centralized control, and industry profits. That said, while some of these alternatives, like Safecast, are much more robust and functional at present than DHS's Cell-All, the restrictive technological protocols being established by DHS and its partners are creating a data enclosure that threatens to defer, perhaps indefinitely, the more laudable vision of a data commons.

References

Adey, P., 2006. 'Divided we move': the dromologics of airport security and surveillance. In: Monahan, T. (Ed.), Surveillance and Security: Technological Politics and Power in Everyday Life. Routledge, New York, pp. 195–208.

Akrich, M., 1992. The de-scription of technological objects. In: Bijker, W.E., Law, John (Eds.), Shaping Technology/Building Society: Studies in Sociotechnical Change. The MIT Press, Cambridge, MA, pp. 205–224.

Altheide, D., 2006. Terrorism and the Politics of Fear. Altamira Press, Lanham, MD.

Andrejevic, M., 2002. The work of being watched: interactive media and the exploitation of self-disclosure. Critical Studies in Media Communication 19 (2), 230–248.

Andrejevic, M., 2007. iSpy: Surveillance and Power in the Interactive Era. University Press of Kansas, Lawrence, Kan.

Andrejevic, M., 2011. The work that affective economics does. Cultural Studies 25 (4–5), 604–620.

Angell, M., 2004. The Truth about the Drug Companies: How They Deceive Us and What to Do About It. Random House, New York.

Associated Press, 2009. South Carolina: Ammonia Cloud Kills Woman. New York Times. <http://www.nytimes.com/2009/07/16/us/16brfs-AMMONIACLOUD_BRF.html> (accessed 17.09.12).

Barnard-Wills, D., 2012. Surveillance and Identity: Discourse, Subjectivity and the State. Ashgate, Burlington, VT.

Barrie, A., 2011. Smartphones Take on Silent Killers as Portable Danger Detectors. Fox News, September 29. <http://www.foxnews.com/tech/2011/09/28/cell-phones-take-on-silent-killers/> (accessed 17.09.12).

Blanchette, J.-F., 2012. Computing as if infrastructure mattered. Communications of the ACM 55 (10), 32–34.

Boddy, T., 2007. Architecture emblematic: hardened sites and softened symbols. In: Sorkin, M. (Ed.), Indefensible Space: The Architecture of the National Insecurity State. Routledge, New York, pp. 277–304.

Böhme, R., Köpsell, S., 2010. Trained to accept?: a field experiment on consent dialogs. In: CHI '10 Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, GA, pp. 2403–2406.

Bulkeley, W.M., 2009. Chicago's camera network is everywhere. The Wall Street Journal. <http://www.firetide.com/assets/0/112/138/9C3A795A-82DD-45CE-8BAD-6409B8BC8774.pdf> (accessed 16.09.12).

Center for Embedded Networked Sensing, 2008. Participatory Sensing, June 4. <http://www.youtube.com/watch?v=t-ItfpA3XiY> (accessed 17.09.12).

Chang, C., 2012. Mobile Air Quality. <http://candychang.com/mobile-air-quality/> (accessed 17.09.12).

Charmaz, K., 2006. Constructing Grounded Theory: A Practical Guide through Qualitative Analysis, second ed. Sage Publications, Thousand Oaks.

Clarke, R., 2009. Privacy impact assessment: its origins and development. Computer Law and Security Review 25 (2), 123–135.

Coaffee, J., 2004. Rings of steel, rings of concrete and rings of confidence: designing out terrorism in central London pre and post September 11th. International Journal of Urban and Regional Research 28 (1), 201–211.

Coaffee, J., Murakami Wood, D., Rogers, P., 2009. The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster. Palgrave Macmillan, Basingstoke, England.

Crang, M., Graham, S., 2007. Sentient cities: ambient intelligence and the politics of urban space. Information, Communication and Society 10 (6), 789–817.

Cuff, D., Hansen, M., Kang, J., 2008. Urban sensing: out of the woods. Communications of the ACM 51 (3), 24–33.

Curry, M.R., Phillips, D.J., Regan, P.M., 2004. Emergency response systems and the creeping legibility of people and places. The Information Society 20, 357–369.

Dennis, S., 2011. Cell-All Program Overview. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Ellerbrok, A., 2011. Playful biometrics: controversial technology through the lens of play. The Sociological Quarterly 52 (4), 528–547.

Finn, R.L., Wright, D., 2012. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Computer Law and Security Review 28 (2), 184–194.

Fisher, J.A., 2009. Medical Research for Hire: The Political Economy of Pharmaceutical Clinical Trials. Rutgers University Press, New Brunswick, NJ.

Fussey, P., Coaffee, J., Armstrong, G., Hobbs, D., 2011. Securing and Sustaining the Olympic City: Reconfiguring London for 2012 and Beyond. Ashgate, Burlington, VT.

Gilliom, J., Monahan, T., 2013. SuperVision: An Introduction to the Surveillance Society. University of Chicago Press, Chicago.

Graham, S., 2010. Cities Under Siege: The New Military Urbanism. Verso, London.

Graham, S., 2012. Digital medieval. Surveillance and Society 9 (3), 321–327.

Graham, S., Wood, D., 2003. Digitizing surveillance: categorization, space, inequality. Critical Social Policy 23 (2), 227–248.

Haggerty, K.D., Ericson, R.V., 2006. The new politics of surveillance and visibility. In: Haggerty, K.D., Ericson, R.V. (Eds.), The New Politics of Surveillance and Visibility. University of Toronto Press, Toronto, pp. 3–25.

Hoffman, D., 2011. Qualcomm Project Presentation. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

King, M., Bailey, C., 2007. Carbon monoxide – related deaths in the United States, 1999–2004. Morbidity and Mortality Weekly Report (CDC) 56 (50), 1309–1312.

Kitchin, R., Dodge, M., 2011. Code/Space: Software and Everyday life. MIT Press, Cambridge, MA.

Klauser, F.R., 2010. Splintering spheres of security: Peter Sloterdijk and the contemporary fortress city. Environment and Planning D: Society and Space 28 (2), 326–340.

Klauser, F.R., Ruegg, J., November, V., 2008. Airport surveillance between public and private interests: CCTV at Geneva International Airport. In: Salter, M.B. (Ed.), Politics at the Airport. University of Minnesota Press, Minneapolis, pp. 105–126.

Koskela, H., 2010. 'Did you spot an alien?' Voluntary vigilance, borderwork and the Texas Virtual Border Watch Program. Space and Polity 14 (2), 103–121.

Li, J., 2011. Nanosensor-Cellphone Integration for Extended Chemical Sensing Network. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Lianos, M., Douglas, M., 2000. Dangerization and the end of deviance. British Journal of Criminology 40 (2), 261–278.

Lyon, D., 2001. Surveillance Society: Monitoring Everyday Life. Open University, Buckingham, England; Philadelphia.

Lyon, D., 2003. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. Routledge, New York. <http://www.loc.gov/catdir/enhancements/fy0650/2002075104-d.html>.

Magnet, S., 2011. When Biometrics Fail: Gender, Race, and the Technology of Identity. Duke University Press, Durham.

Monahan, T., 2010a. Surveillance as governance: social inequality and the pursuit of democratic surveillance. In: Haggerty, K.D., Samatas, M. (Eds.), Surveillance and Democracy. Routledge, New York, pp. 91–110.

Monahan, T., 2010b. Surveillance in the Time of Insecurity. Rutgers University Press, New Brunswick.

Monahan, T., Mokos, J.T., 2010. Sensing environmental danger in the city. International Review of Information Ethics 12, 21–27.

Monahan, T., Palmer, N.A., 2009. The emerging politics of DHS fusion centers. Security Dialogue 40 (6), 617–636.

Montagnino, J., 2012. NC4 Situational Readiness Solutions to Manage Risks. <http://www.nc4.us/> (accessed 09.09.12).

Murakami Wood, D., 2007. Pervasive Surveillance: Enabling Environments or Embedding Inequalities. Workshop on Surveillance and Inequality. Arizona State University.

Murakami Wood, D., 2009a. Chicago: The Future of US CCTV? Notes from the Ubiquitous Surveillance Society. <http://ubisurv.wordpress.com/2009/02/21/chicago-the-future-of-us-cctv/> (accessed 07.06.11).

Murakami Wood, D., 2009b. Where Will the Big Red Balloons Be Next? Notes from the Ubiquitous Surveillance Society. <http://ubisurv.wordpress.com/2009/12/04/big-red-balloon/> (accessed 16.09.12).

Murakami Wood, D., Webster, C.W.R., 2011. The normality of living in surveillance societies. Innovating Government 20 (3), 151–164.

Needs, C., 2011. NC4 Project Presentation. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Neighborhood Link, 2010. How Landlords Can Use Credit Scoring to Make Rental Decisions. <http://www.neighborhoodlink.com/article/Homeowner/Credit_Scoring_Rentals> (accessed 19.07.11).

O'Harrow, R., 2005. No Place to Hide. Free Press, New York.
Ottinger, G., 2010. Constructing empowerment through interpretations of environmental surveillance data. Surveillance and Society 8 (2), 221–234.
PBS NewsHour, 2011. Safecast Draws on Power of the Crowd to Map Japan's Radiation, November 10. <http://www.pbs.org/newshour/bb/science/july-dec11/japanradiation_11-10.html> (accessed 17.09.12).
Rula, J., Bustamante, F.E., 2012. Crowd (soft) control: moving beyond the opportunistic. In: Proc. of the Thirteenth Workshop on Mobile Computing Systems and Applications (HotMobile), San Diego, CA.
Safecast, 2012. Safecast. <http://blog.safecast.org/> (accessed 17.09.12).
Shilton, K., 2009. Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. Communications of the ACM 52 (11), 48–53.
Shilton, K., 2012. Participatory personal data: an emerging research challenge for the information sciences. Journal of the American Society for Information Science and Technology 63 (10), 1905–1915.
Synkera Technologies, 2011. Chemical Sensors for Mobile Devices. <http://www.synkera.com/sensors/chemical-sensors-for-mobile-devices.html> (accessed 19.09.12).
The Impact Project, 2012. Trade, Health and Environment Impact Project. <http://theimpactproject.org/index.html> (accessed 17.09.12).
Thrift, N., French, S., 2002. The automatic production of space. Transactions of the Institute of British Geographers 27 (4), 309–335.
U.S. Department of Homeland Security, 2007. Cell-All Ubiquitous Biological and Chemical Sensing. <https://http://www.fbo.gov/index?s=opportunity&mode=form&id=f292c1fdbd46777a3ff8ca64ef96658f&tab=core&_cview=1> (accessed 17.09.12).
U.S. Department of Homeland Security, 2010. Cell-All: Super Smartphones Sniff Out Suspicious Substances. <http://www.dhs.gov/cell-all-super-smartphones-sniff-out-suspicious-substances> (accessed 17.09.12).
U.S. Department of Homeland Security, 2011a. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).
U.S. Department of Homeland Security, 2011b. Privacy Impact Assessment for the Cell All Demonstration. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_s&t_cell_all.pdf> (accessed 19.09.12).
U.S. Department of Homeland Security, 2011c. Transcript of the Meeting of the Data Privacy and Integrity Advisory Committee. May 19. <http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy_dpiactranscript_may192011mtg.pdf> (accessed 17.09.12).
Verrico, J.S., 2011. Welcome and Opening Remarks. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).
Wall, T., Monahan, T., 2011. Surveillance and violence from afar: the politics of drones and liminal security-scapes. Theoretical Criminology 15 (3), 239–254.
Weber, J., 2011. Techno-security, risk and the militarization of everyday life. In: Conference on "The Computational Turn: Past, Presents, Futures?". Aarhus University, pp. 168–173.
Whitson, J.R., Haggerty, K.D., 2008. Identity theft and the care of the virtual self. Economy and Society 37 (4), 572–594.
Winner, L., 1986. The Whale and the Reactor: A Search for Limits in an Age of High Technology. University of Chicago Press, Chicago.
Woodhouse, E., Hess, D., Breyman, S., Martin, B., 2002. Science studies and activism: possibilities and problems for reconstructivist agendas. Social Studies of Science 32 (2), 297–319.