THE INFORMATION SOCIETY
2016, VOL. 32, NO. 4, 229–240
http://dx.doi.org/10.1080/01972243.2016.1177765

Routledge
Taylor & Francis Group

Built to lie: Investigating technologies of deception, surveillance, and control

Torin Monahan

Department of Communication, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, USA

ABSTRACT

This article explores technological systems that dissimulate by design. Examples include untrustworthy hotel and workplace thermostats, digital applications to spy on workers and family members, and commercial and law-enforcement systems that surreptitiously collect mobile phone data. Rather than view such cases as exceptional, I argue that deceptive communication systems are hidden articulations of normal technological orders. If deception in itself is not the primary problem with such systems, then transparency alone cannot be the solution. As troubling as institutional opacity might be, an analysis of deceptive systems reveals more fundamental problems: imbalances in power and widespread acquiescence to corporate and state efforts to control individuals, groups, and their data. By moving beyond a quest for (or belief in) technological veracity, scholars could redirect attention to power inequalities and the pressing question of how to live together ethically.

ARTICLE HISTORY
Received 19 October 2015
Accepted 11 February 2016

KEYWORDS
Communication; dark side; deception; malware; surveillance

In the midst of what has been called a "big data revolution," critical scholarly attention has understandably turned to the foreboding implications of this trend for individual privacy, human autonomy, and social justice (Lyon 2014; Mosco 2014). If patterns in disparate forms of data can accurately predict individual or group properties, then this encourages decision making based on those predictions. The results could foster massive invasions of privacy and intensified discrimination, all normalized as rational forms of risk management on the part of individuals and institutions, or these changes could lead to progressive societal transformations, as the most vocal utopian-minded supporters of big data believe (e.g., Mayer-Schönberger and Cukier 2013). Big data is wrapped up in these dystopian and utopian mythologies (boyd and Crawford 2012), which encourage a belief that one's tastes, behaviors, disease propensities, beliefs, sexual orientation, racial identity, and likelihood of personal success or failure can all be read from the crystal ball of big data; the difference lies in whether one views this as an enabling or disabling capability. Either way, the veracity of such predictions made from data is either unquestioned or seen as beside the point.

Similarly, marketing discourses about the unreliability of individual self-reporting reinforce perspectives of the relative trustworthiness of data derived through technologically mediated processes. Thus, what is known as "neuromarketing" relies on somatic responses (e.g., heart rate, pupil dilation, respiration, brain waves), measuring individuals' responses to stimuli, such as exposure to a product, without the need for verbal communication (Andrejevic 2013; Murakami Wood and Ball 2013). Likewise, billboards and store displays are being designed to track the movement and focus of customers' eyes, generating data about individual attention and tastes of which the person may be completely unaware and therefore unable to disclose accurately even if he or she were cooperative (Owano 2013; Tobii 2015). These developments signal, on one hand, that people do not have privileged or reliable access to their internal processes, and, on the other hand, that "the body does not lie," provided that one has the proper instruments to read its somatic markers and precognitive secrets (Aas 2006). As with discourses about big data, this suggests that organizations with access to systems for reading the body may have greater—and possibly more accurate—knowledge of one's preferences or likely behaviors than the individual in question has. Technologically derived truths, as such, are not called into question.

Scholars in the field of science and technology studies have long deconstructed myths of technological neutrality and inevitability (Akrich 1992; Bowker and Star 1999; Oudshoorn 1999; Winner 1980), whereas the present moment may require more attention to the fallacy of technological veracity. The truth regimes of big data and

CONTACT Torin Monahan torin.monahan@unc.edu Department of Communication, University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA.

sensing systems are always based on necessarily reductive models of reality. Although they may "work" to bring about effects based on unknown causal chains (Andrejevic 2013; Mayer-Schönberger and Cukier 2013), they are accurate only to the extent that those models or representations are imposed successfully back upon the social systems they describe. Thus, "data doubles" of individuals become problematic especially when institutions make decisions based on those partial, limited, and necessarily biased representations (Haggerty and Ericson 2000) or when people come to see themselves through those identity constructs (Browne 2015). "Big data" representations of reality do not at long last achieve positivistic dreams of isomorphic correspondence between a model and the world, yet their ramifications can be profound if institutions internalize their logics and are transformed in their likeness to privilege the classifiable and calculable. Then again, beyond such academic observations about the limitations and politics of representation, it must be acknowledged that many technological systems are deliberately built to lie.

In this article, I investigate a number of technological systems that dissimulate by design. Examples can include things like Volkswagen's so-called clean diesel cars that were equipped with software designed to fool emissions testing by misrepresenting actual pollution released by the vehicles when not being tested (Plumer 2015). Similarly, many hotel and business thermostats are decoys that give incorrect readings to occupants and provide a false sense of individual control (Sandberg 2003). Casino video slot machines are programmed to present a statistically improbable number of "near misses" and deliver frequent small payouts to lend the impression that gamblers are winning even when they are losing badly (Schüll 2012). In a different vein, while mobile phones might appear transparent in their functions, hidden apps can allow parents (or others) to monitor their children's locations, text messages, and calls, all without divulging that functionality (e.g., TeenSafe 2015). The police also use "Stingray" systems to spoof cell-phone towers so that mobile phones provide users' locations (and perhaps more) without either the phone or the user having any awareness of that action (Farivar 2014). Keystroke-tracking software and other workplace surveillance systems operate in a similar way: seeming to respond solely to workers, while actually communicating to managers (Introna 2000; Kiss and Mosco 2005). Even some household devices such as smart televisions are recording users' viewing habits, facial features, and spoken words, ostensibly to provide better service, but also to amass potentially profitable data for companies (Harris 2015). For the majority of cases, the term *function creep* is insufficient to describe these practices. The systems have not simply been appropriated for uses that were not originally intended, but instead have multiple, simultaneous, intentional functions of which not all users may be aware.

Ranging from the seemingly mundane to the extraordinary, together these examples illustrate some fundamental dimensions of "untrustworthy" systems. First, most are polyvalent and polyvocal: They lend the outward appearance of having a single primary function and audience, but they in fact have multiple hidden functions and audiences. Second, and related, especially in their hidden functionalities, these are surveillance systems. Most are designed to generate information about and facilitate control of users. For instance, things like deceptive hotel thermostats are programmed to report room occupancy to hotel management, at the same time that they control the behavior of guests and forestall complaints by implying that discomfort has no objective external cause. Third, untrustworthy technologies are commonplace and often legal. Thus, innovative privacy activists have built similar spoofing systems that introduce "noise" into databases to hinder user profiling (Brunton and Nissenbaum 2011), and criminals might deploy similar systems and tactics for financial gain (e.g., by using Trojan horses, phishing, pharming) (Whitson and Haggerty 2008; Cole and Pontell 2006), whereas untrustworthy systems should be seen as ordinary and theorized as such.

The goal of this article, therefore, is to ask what can be learned by approaching such systems not as aberrations but as hidden articulations of normal technological orders. The gap between expectation and actuality serves as a space of politics, as a site for tracking shifting power relationships and cultural norms, and also for contesting those changes. If there are multiple scripts for each technological system, then transparency with regard to hidden functions could never serve as a corrective in itself because the inherent politics and conflicts would necessarily remain (Brucato 2015; Han 2015; Monahan 2015).[1] Instead of focusing on whether a system is lying or telling the truth, it is perhaps more important to ask what growing technological practices of concealment say about issues of surveillance and trust in society. Accepting that technological veracity is always a fallacy and that untrustworthiness is the norm for all technological systems could redirect attention to power inequalities and the pressing question of how to live together ethically.

A detour through ritual and the dark side

To focus on the deceptive aspects of technologies alone would suggest that they fail to communicate honestly and sincerely. They intentionally withhold information

or yield incorrect information, thereby fracturing the communicative chain. However, the mechanistic transmission model upon which this evaluation is based ignores—or subordinates—the deeper cultural and social aspects of communication. James Carey famously used the term "ritual" to describe this different and arguably more fundamental function of communication: "A ritual view of communication is directed not toward the extension of messages in space but toward the maintenance of society in time; not the act of imparting information but the representation of shared beliefs" (Carey 1992, 18). From this perspective, communication entails the ongoing construction of the world through the creation and deployment of symbolic forms. As such, communication is also an inherently social and material endeavor, giving rise to and dependent upon ideologies, subjectivities, political economies, infrastructures, and organizational forms (Gates and Magnet 2007; Leonardi 2012; Mumby 2005; Packer and Wiley 2012). Thus, instead of seeing deceptive technologies as failing to transmit effectively, one could seek to learn about the problematics of contemporary social and material worlds through the study of such devices.

Better communication is often presented as the solution to just about any disagreement or antipathy, from the level of tensions in romantic relationships all the way to conflicts between nations. Failures to communicate effectively, however, are both endemic and potentially salutary. As John Durham Peters explains:

> Why others do not use words as I do or do not feel or see the world as I do is a problem not just in adjusting the transmission and reception of messages, but in orchestrating collective being, in making space in the world for each other. Whatever "communication" might mean, it is more fundamentally a political and ethical problem than a semantic one.…The ultimate futility of our attempts to "communicate" is not lamentable; it is a handsome condition. (Peters 1999, 30–31)

As with the ritual view of communication, this orientation implies that people should not aspire to eliminate noise and difference, to perfect "the transmission and reception of messages," but instead see communication as an ongoing and never complete "project of reconciling self and other" (Peters 1999, 9). Misunderstanding, from this view, signifies diverse human and cultural richness and introduces untapped opportunities for communing with others, for making the world a more just and rewarding place. Romantic as this notion might be, it does complicate interpretations of deceptive transmissions and points toward the need for ethical and political adjustments, not necessarily more accurate or truthful systems.

Although such views of communication as ritual or culture might imply studies of collaborative symbolic practices, they can also afford inquiry into power differentials and social inequalities (e.g., Sharma 2014; Couldry 2003), especially if one takes a symmetrical approach and analyzes dysfunction as similarly revealing of social orders. What has been termed "the dark side" of communication could assist with this investigation. As Spitzberg and Cupach (2011b) describe, the dark side signifies a host of remarkably common uses of interpersonal communication for purposes other than generously connecting or sharing with others: bullying, threatening, deceiving, harassing, rejecting, expressing anger, eliciting guilt, hurting feelings, and so on. While the concentration is on the harmful, destructive, and repulsive, such practices can also have "prosocial" intentions or outcomes; for instance, lying is often seen as a way to protect someone from the harm that the truth could cause (Spitzberg and Cupach 2011b). Similarly, while expressing anger might be socially coded as negative, it can also bring about positive social or organizational changes as people respond to it (Spitzberg and Cupach 2011b). For these reasons, "the dark side [of communication] is shown to be deeply concerned not only with dysfunction, but also with social processes marked by functional and normative ambivalence" (Spitzberg and Cupach 2011a, xiii).

What "ritual" and "dark side" treatments of communication share in common is the view that communication is a social and symbolic act that cannot be reduced to mechanistic models of transmission. Communicative failures or tensions are meaningful and call out for analysis beyond surface observations of their existence. Technologies are also active participants in these dramas: They embody the conditions and values of their creation, structure the conditions for human action and interaction, and acquire new meanings and purposes as others negotiate them (Pfaffenberger 1992; Monahan 2010; Slack and Wise 2005; Winner 1986). Taking inspiration from John Durham Peters, deceptive communication technologies can be read as both ubiquitous and consequential, as presenting political and ethical challenges that demand attention.

For your comfort

Digital thermostats for climate control systems present a fruitful starting point for such analysis because of their seeming innocuousness.[2] Thermostats are prototypical transparent technologies that present information about one's enclosed environment—typically temperature, but also humidity or other variables—and enable user control over heating, air conditioning, and ventilation (HVAC) units designed to alter that environment. A breakdown in

that feedback loop would usually be interpreted as technical malfunction or inability, not calculated deception. However, especially in hotels or office spaces, thermostats afford unseen manipulation of occupants and can cultivate individual psychological insecurity if occupants come to see their discomfort as ungrounded with no external reason for it. Thermostats may serve as an outward symbol of hospitality while having the opposite effect on functional and experiential levels.

So-called smart thermostats and meters are advertised for their energy and cost-saving abilities, as they predict energy use, ration access to it, dynamically adjust to needs, and eliminate what is perceived to be unnecessary heating or cooling (e.g., of vacant rooms, floors, or buildings). Although there is some disagreement about the effectiveness of such systems for reducing energy consumption in less predictable settings, such as college dorms (Woolley et al. 2014), the market for high-tech "property management systems" and "energy management systems" in the hospitality industry is clearly fueled in part by a managerial desire for centralized, remote observation and control, whether of properties, employees, or customers. As one vendor of such systems explains:

> We believe that one of the major factors in almost all hotel environments is the lack of visibility your hotel maintenance staff has into how your hotel HVAC resources are performing. …We enable your Facilities managers to see exactly what is going on in any area that has our solution installed. (Pelican Wireless Systems 2011, online)

In this context, surveillance-based thermostats that actively detect and adjust to room occupancy through the use of motion sensors, door sensors, sound sensors, CO_2 sensors, and key-card detection systems are viewed as essential management tools (Grochmal 2013; Schneider Electric 2015). While the goal may be one of complete transparency, the audience for such messages is management, not occupants of those spaces, be they customers or custodial staff.

As with other surveillance systems, visibility invites—or cultivates a desire for—control through techniques of intervention (Cohen 2008a; Staples 2014). One company makes the connection between monitoring and active control explicit: "EvolveNet is Evolve Guest Controls' software that gives the front desk and engineering the ability to monitor and control the lighting and temperature of each room, wing, floor, or the entire facility remotely" (Hasek 2011, online). Observation and control can have direct associations of detecting a specific problem and then remotely addressing it, but the technological imperative tends toward the creation of all-encompassing occupant surveillance systems:

> Through a secure IP address, users can easily scroll though energy usage data by room, floor or even the entire facility, with the ability to make manual adjustments to settings when required. Millions of data points are captured to create customized reports tailored to the needs of your facility. Reports or alerts can also be sent to a mobile device or inbox to enhance response time if problems arise. (Schneider Electric 2010, online)

Although the aspiration may be predictive and completely automated management of facilities, such as initiating cooling once customers check in but before they arrive at their room or turning the thermostat up when people leave for the day, this invariably relies on monitoring of occupants, especially through sensors, to determine their presence or absence in rooms. It is about watching and controlling people, and particularly their interaction with and experience of the environment.

For this discussion, a key component of controlling occupants in space is providing them with a semblance of control, no matter how spurious that might be. According to *The Wall Street Journal*, "HVAC experts acknowledge what millions of office workers have suspected all along: A lot of office thermostats are completely fake—meant to dupe you into thinking you've altered the office weather conditions" (Sandberg 2003, online). In their attempts to achieve verisimilitude, engineers have even equipped thermostats with pneumatic devices so that they emit a completely ineffectual but satisfying "hiss" when someone adjusts them (Arabe 2003). That sound is the communicative equivalent of a sign index (Cobley 2001), such as smoke meaning fire, except that it is a false one. Such placebo thermostats, as with the numerous placebo buttons to request a "walk" signal at pedestrian crosswalks, "close doors" in elevators, or "open doors" in subway cars (Baraniuk 2015; Sandberg 2003), are intended to instill an "illusion of control" in people so that they feel a sense of individual empowerment and social solidarity with others around them (Langer 1975). In terms of the dark side of communication, these devices may have the potential to achieve psychological benefits through deceptive means. In hotel or apartment contexts, thermostats tend to miscommunicate in slightly different ways: they have a limited range of adjustment, implying that such a range is sufficient for most people, and they can be "calibrated" to display an incorrect reading (CresendoCrook 2015). These design features expertly achieve social control for most people by combining insecurity (e.g., "It must just be me") with a false sense of ability.[3]

Deceptive thermostats reveal a great deal about individual–institutional power imbalances, data imperatives, and trust relationships. Through the use of these devices, businesses tacitly assert the right to mislead, monitor,

and control customers or employees in the name of perceived efficiencies. By implementing placebo buttons, temperature limits, and inaccurate readouts, management evokes a sense of individual psychological insecurity, executed through a kind of paternalistic obligation to discipline individuals who might not set temperature levels responsibly. By flagging these messages, I do not aim to refute or affirm the position that individuals would not behave rationally or responsibly. Rather, I would like to draw attention to the ways that what is considered rational and responsible becomes equated with managerial data collection, oversight, and control, which are then delegated to technological devices to enforce. Moreover, as some hotel thermostats now have "green" buttons that customers can push to voluntarily submit to less comfortable, but ostensibly less wasteful, temperature settings (Honeywell 2015; Baral 2012), it is clear that such devices are being harnessed to transform existing norms in overt ways. This will likely lead to even greater inequalities in treatment, which happens already when individuals on "budget" electricity plans are charged higher rates or have their air-conditioning systems overridden remotely during peak heat spells (Gilliom and Monahan 2013). Through such surveillance systems, a voluntary choice today can rapidly become a demand unequally applied tomorrow.

Institutional malware

When individuals attempt to gain access surreptitiously to one's personal data for their own profit, it is typically called identity theft. But beyond the well-publicized threats of email phishing scams, credit card theft, and system hacks resides a host of spyware applications circulated by supposedly reputable institutional actors, such as corporate workplaces, police agencies, and technology companies. Given the media-fueled moral panics surrounding identity theft (Cole and Pontell 2006; Monahan 2009), it is instructive that the growing use of institutional malware receives such scant notice. Apparently, deceptive technologies are subject to differential evaluation and judgment based upon the relative status and perceived agenda of the entity implementing them.

Workplaces represent one of the key sites for widespread implementation of spyware. In the United States, it is estimated that roughly 75 percent of employees are electronically monitored at work, especially through computer, mobile phone, and tablet applications (Ball 2010; Gilliom and Monahan 2013). This can include the tracking of computer keystrokes, e-mails, chats, Web browsing, phone conversations, physical location, mouse clicks, and more. Although spyware companies and business magazines recommend informing employees of such practices, including providing information about the scope of monitoring and clear guidelines for acceptable and unacceptable behavior, many—and perhaps most—companies do not do so (Alder, Ambrose, and Noel 2006; Kiser, Porter, and Vequist 2010). As a result, the systems that many employees use to perform their work tasks are deceptive. They communicate functionality that is directed by a single user, namely, the employee, but in reality there are multiple users (managers, information technology [IT] staff, auditors) who can access performance data and personal communications at any time.

In business literature and spyware marketing materials, employee monitoring of this sort is discursively framed as necessary, responsible action on the part of companies. For instance, one *PC World* article argues:

> Do you know what your employees are doing on the Web? At a minimum, they're probably goofing off watching YouTube videos. At worst, they could be steering your company toward financial ruin … gone are the days when PC monitoring was an optional, draconian security measure practiced only by especially vigilant organizations. Today, more than three-quarters of U.S. companies monitor employee Internet use. If your business is in the remaining quarter that doesn't do so, you're probably overdue for a policy change. (Strohmeyer 2011)

Spying on employees is presented as conscientious management to increase productivity, avoid lawsuits, and keep data secure (Strohmeyer 2011, online). In order for this logic to hold, though, employees must simultaneously be perceived as untrustworthy and in need of oversight. One spyware company, My Team Monitor, communicates this through a promotional video that depicts workers as monkeys who are closely watched and carefully trained, through incentives for productivity (bananas) or threats for idleness (angry gorillas) (My Team Monitor 2013b). By dehumanizing workers in this way, the video implies that workers are naturally unintelligent and lazy, and therefore in need of a wise, diligent trainer to ensure their success.

This viewpoint has a long pedigree in the history or workplace surveillance, as Frederick Winslow Taylor, the father of "scientific management," told a similarly insulting anecdote about a short, uneducated foreign laborer, "Schmidt," who supposedly eagerly increased his productivity under a system of financial incentives (piecework) and managerial oversight. In Taylor's words:

> Now one of the very first requirements for a man who is fit to handle pig-iron as a regular occupation is that he shall be so stupid and so phlegmatic that he more nearly resembles in his mental make-up the ox than any other type. … He is so stupid that the word "percentage" has

> no meaning to him, and he must consequently be trained by a man more intelligent than himself into the habit of working in accordance with the laws of this science before he can be successful. (Taylor 1911; cited in Wrege and Perroni 1974, 17)

Although Schmidt, whose real name was Henry Noll (Wrege and Perroni 1974), was aware of the observation he was under, contemporary workers are visible in many less obvious ways. As My Team Monitor recounts:

> One of our most popular features is the employees' screenshots. You can view screenshots taken throughout a specific day and even flag screenshots containing non-work-related activities. If you were looking for a bit more detail, you can view an activity chart, which logs your employees' working time, key presses, and mouse clicks. (My Team Monitor 2013a, video)

Additionally, workers may be constructed as dumb or lazy, whereas managers are presented as hard-working, analytically capable individuals who deserve to monitor others as a form of leisure akin to watching a sports game at home. Thus, another company, InterGuard, offers a marketing video that depicts a manager, in animated form, sitting tilted back in a chair with his hands behind his head watching a computer monitor displaying his workers' activity. The voice-over says, "Instead of monitoring systems, InterGuard records users at the end point, which is where the critical action takes place. It's like having surveillance cameras installed in your PCs, so you get to see everything that happens just as clearly as watching a replay" (InterGuard 2015, online). Deceptive workplace technologies clearly rely on the creation and circulation of simplistic, yet effective, identity constructs that normalize unequal treatment and rights.

Beyond workplaces, many parents spy on children, and intimate partners (or ex-partners) spy on each other with surprising regularity (Gregg 2013; Marx and Steeves 2010; Mason and Magnet 2012). In one disturbing development, though, police agencies throughout the United States have had a hand in purchasing and distributing to parents hundreds of thousands of copies of a malware program called ComputerCOP (Maass 2014). The stated goal of this program is to help parents monitor their children's use of the Internet, including Web browsing, e-mailing, and chatting, to protect them from online predators. In actuality, the program relies on an incredibly vulnerable keystroke monitoring function that does not discriminate between adult or child users and introduces a host of data vulnerabilities, perhaps exposing users to the very threats it purports to block. According to the Electronic Frontier Foundation, which conducted an investigation into ComputerCOP, the keystroke monitoring function:

> could place a family's personal information at extreme risk by transmitting what a user types over the Internet to third-party servers without encryption. That means many versions of ComputerCOP leave children (and their parents, guests, friends, and anyone using the affected computer) exposed to the same predators, identity thieves, and bullies that police claim the software protects against. (Maass 2014, online)

The software itself is deceptive in the sense that child or adult users may be unaware that by using their computer they are simultaneously generating data for a hidden surveillance application on the computer. Although a technologically savvy user might come to the same conclusion about most Internet applications and websites, the difference here is that family members are the ones installing the application, with encouragement from law enforcement, to spy on—and potentially endanger—their loved ones.

ComputerCOP is deceptive in other ways too. The company claims false endorsements from the American Civil Liberties Union (ACLU) and the U.S. Department of Treasury and references a long-expired endorsement from the National Center for Missing and Exploited Children (Maass 2014). The reason for its remarkable success, including its purchase by hundreds of police agencies in 35 states (at up to $42,000 per agency), has to do with its tailored marketing to police agencies looking for positive public relations fodder and legal ways to spend funds obtained from seized assets and other sources (Maass 2014). By buying thousands of copies of the software to distribute to their communities for free, police agencies receive branded versions of the software that advertise the specific agency and can even include a photograph of the local police chief (Maass 2014). This can obviously boost the reputation of police agencies and assist chiefs with reelection, regardless of how ineffective or dangerous the software may be.

As one final example of everyday institutional malware, the software company Adobe released in 2014 a version of its e-reader, "Digital Editions," that siphoned up information about users' reading habits and sent it to Adobe. This happened without the consent of users and without disclosure by Adobe. Anyone using the e-reader unwittingly revealed the titles of books they opened, the number of pages read, and the time spent reading (Quintin 2014). More than that, metadata were collected on all the books in users' libraries and on any connected e-book readers, such as Nook, Kindle, or Boyue, even if Adobe Digital Editions never opened those books (Quintin 2014). This practice was deceptive in the general way that most websites or digital rights management (DRM) systems are: They hide the fact that they are surveillant. But Adobe circulated privacy statements that were

definitively false, claiming, for instance, that information collected pertained only to "the eBook currently being read by the user and not for any other eBook in the user's library or read/available in any other reader" (Quintin 2014, online). The final *coup de grâce* was that Adobe was sending these private and potentially sensitive data in unencrypted plain text format over the Internet. As Nate Hoffelder, who is the person who brought these revelations to light, explained: "Adobe is not only logging what users are doing, they're also sending those logs to their servers in such a way that anyone running one of the servers in between can listen in and know everything" (Hoffelder 2014, online).

Adobe responded to the negative feedback generated by these revelations by releasing an updated version of the e-reader. This new version appeared to solve the problems by ensuring that data were encrypted and sent over secure servers, as well as ceasing the collection of data not relevant to DRM checks (Quintin 2014). However, it remains unclear whether Adobe engaged in the initial privacy violation intentionally. What is certain is that the data were not being collected to improve services for users, but instead were intended to "facilitate the implementation of different licensing models by publishers" (Quintin 2014). Users' data, in essence, were being captured and traded as valuable commodities without the awareness or remuneration of users. Similar discoveries have also been made about LG Smart Televisions, which collected and insecurely downloaded metadata on owners' viewing habits (Cushing 2013; Hoffelder 2014), so these practices are poised to continue, in some form or another, because the technical systems enable it, data markets encourage it, and regulators tend to ignore it (Cohen 2012; Pasquale 2015).

These examples of institutional malware illustrate how power asymmetries between institutional actors and individuals have the effect of normalizing deception on the part of the relatively powerful. When businesses or police agencies insist on using malware applications, it is done under the banners of sound business management (with workplace surveillance) or necessary public safety (with police-distributed software). Even Adobe's e-reader fiasco, which was illegal and patently unethical, underscores the dominant logics of the technology industry: toward surreptitiously collecting and trading user data for financial gain, while hiding behind official rationales of improving services and protecting intellectual property (Arditi 2013; Cohen 2008b; Pasquale 2015). People face greater privacy risks from institutions than from individual criminals (Monahan 2010; Regan 2003), yet other than high-profile disclosures such as dragnet surveillance by the National Security Agency (Lyon 2015), deceptive surveillance on the part of institutions is seldom discussed or problematized.

Decoys in the data hunt

Trashcans on the street. Phone booths on the corner. Planes flying overhead. In the emerging world of smart cities and the Internet of things, everyday objects are much more than they seem. As with other deceptive technologies, it is not simply the case that these artifacts cease to function in their assumed role. Rather, they use their outward appearance and assumed singular functionality as decoys to enmesh people in surveillance encounters. As with the best of decoys, most people are unaware of the dissimulation and fail to see the extent to which their data are being captured.

Although homes are increasingly populated with smart gadgets that can report sensitive personal information (Fitchett and Lim 2008; Morozov 2013), in public places it is typically mobile phones that promiscuously connect with other devices to reveal the identity or habits of individuals. For example, in 2013 trash bins in London managed by the advertising company Renew were equipped with WiFi receivers to invisibly capture the unique identification information of all mobile phones in the area. The capturing system, called Presence Orb, catalogued phone make, serial number, signal strength, and speed of movement, enabling the company to identify patterns in individual behavior over time (Campbell-Dollaghan 2013). Renew's chief executive officer (CEO) boasted, "We will cookie the street" (CBS/AP 2013), which is an allusion to the way that websites track individuals and their browsing habits over time by installing hidden "cookies" of computer code on users' machines. In a single week of testing, Renew was able to track "more than four million devices … peaking at 946,016 devices detected in a single day. And that's just from 12 Orb-enabled trash cans in central London" (Campbell-Dollaghan 2013, online). The ultimate goal will be to determine fine-grained behavioral patterns of individuals—such as where they shop, which trains they take, when they get lunch—so that Renew could sell access to those data for other companies to deliver customized ads to pedestrians (Campbell-Dollaghan 2013). After a public backlash concerning the testing of such "spy bins," the City of London Corporation, which manages the area in question, claimed that it was completely unaware and did not approve of the data collection, so it ordered Renew to shut them down (CBS/AP 2013).

The company Titan360 deployed a similar system in New York City with hundreds of public payphones displaying its ads. The payphones were equipped with

hidden "smartphone-sniffing beacons" that detected Bluetooth apps on people's phones and sent tailored ads to them (Dwoskin 2014). For instance, when individuals downloaded the Tribeca Film Festival app, if they passed by a Titan360 phone booth, they would be sent information about other films screening near them (Dwoskin 2014). The partnering company, Gimbal, then drew upon this expanded network of beacons to approach local businesses and sell access to cell phone users in their radius (Dwoskin 2014). Although the Titan360 system apparently collected less data than the Renew trash bins, the city was similarly unaware of the practice. In Titan360's case, the company lied to the city about the functionality, saying that the beacons would be used solely for maintenance purposes—to alert employees when to change outdated ads (Dwoskin 2014). After the city ordered the company to cease collecting mobile phone data, as well as selling to advertisers access to mobile phone users, Titan360's Executive Vice President admitted, "We overstepped," and claimed that it was simply the result of a misunderstanding (Dwoskin 2014).

Law enforcement is also actively collecting mobile phone data by covert means. In vehicles and airplanes across the United States, police agencies have installed International Mobile Subscriber Identity (IMSI) catchers to scoop up unique identifying information and locations of all mobile phones in the area. The systems work by mimicking cell phone towers with the strongest possible signal strength, even though they are not cell towers nor do they actually have the strongest signal (Barrett 2014). By dint of mobile phone protocols, this forces all proximate phones to connect to the IMSI catcher and communicate their data, unknown to the owner, before being cycled off to an actual cell tower. The effect is comparable to what is known as a "man in the middle" form of computer hacking, where "a person's electronic device is tricked into thinking it is relaying data to a legitimate or intended part of the communications system" (Barrett 2014, online). Moreover, the ability exists for such systems to jam cellular signals or download phone data (e.g., e-mail, contacts, photographs), although it is unknown whether police agencies have exploited this functionality (Barrett 2014). While thoroughly deceptive, the systems are attractive to law enforcement because they circumvent telecommunication companies altogether, so there is no need to partner with them or obtain warrants to request information from them (Barrett 2014). That said, the systems are probably illegal—as the ACLU has argued—because they collect data on everyone in their territory, whether or not they are making a phone call, including people in private spaces such as buildings or houses, not just people under investigation (Gillum, Sullivan, and Tucker 2015; RT.com 2014). Even for people under investigation, there is evidence that police do not obtain probable-cause warrants for the use of IMSI catchers (Zetter 2014).

The IMSI catcher that has received the most attention to date is called Stingray (Farivar 2014). Police agencies across the United States rely on them, but it is incredibly difficult to obtain details because they obfuscate by denying such use or insist that any information about their use is confidential or classified. Regardless, the ACLU has been able to confirm their deployment by "60 agencies in 23 states and the District of Columbia" (American Civil Liberties Union 2015, online). It has been reported that the Chicago Police Department has used Stingray systems to listen to the voice calls of activists, too (Handley 2014). In one remarkable case, public records indicated that the police department in Sarasota, FL, had used Stingrays at least 200 times without obtaining any judicial approval because "the device's manufacturer made the police department sign a non-disclosure agreement that police claim prevented them from disclosing use of the device to the courts" (Zetter 2014, online). After the ACLU received legal approval to review the police department's Stingray-related documents, the federal U.S. Marshals Service, in an unprecedented move, confiscated them at the last minute and refused to allow such access (Doctorow 2014). The ACLU summarized the move: "We've seen our fair share of federal government attempts to keep records about stingrays secret, but we've never seen an actual physical raid on state records in order to conceal them from public view" (Zetter 2014, online).[4]

More powerful than Stingrays, though, are airplane-mounted IMSI catchers known as "dirtboxes." According to one report, by flying over urban areas, "the technology in the two-foot-square device enables investigators to scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location" (Barrett 2014, online). Evidence suggests that the FBI is the primary agency conducting such surveillance flights, which include high-resolution video and photographic surveillance as well, with more than 100 planes flying over 30 cities across the country (Gillum, Sullivan, and Tucker 2015). As discovered through investigative journalism by the Associated Press, the FBI has gone to great lengths to keep the flights secret, including establishing at least 13 shell companies with different names and no physical location to mislead curious individuals (Gillum, Sullivan, and Tucker 2015). The planes were even used to monitor Black Lives Matter activists in Baltimore, MD, who were protesting the death of Freddie Gray while in police custody (Gillum, Sullivan, and Tucker 2015), which would appear

to be an infringement on First Amendment-protected freedom of speech and assembly.

IMSI-catcher systems like Stingrays and dirtboxes weave multiple webs of deception. First, without close scrutiny, they appear to be ordinary vehicles or airplanes in the world. Second, airplanes are registered to shell companies to jumble any paper trail that could identify their true function. Third, their technical protocols mislead mobile phones into thinking that they are connecting to regular cellular towers and that those towers are transmitting the strongest signal. Fourth, records about IMSI systems are hidden from public scrutiny, sometimes through extreme means, while authorities deny the existence or extent of such systems. Fifth, police claim to obtain necessary warrants for such surveillance, but records show that they interpret nondisclosure agreements with technology vendors as superseding legal requirements for police investigations. Although all communication devices may have built-in deceptive valences, in this case a great deal of labor goes into accentuating those functions and ensuring that they remain obscured.

The systems just reviewed illustrate some facets of what this section referred to as "the data hunt." The hunt metaphor may be a useful one for thinking about the various tricks deployed and justified by institutional actors for securing data on individuals and on entire populations. Although there has been some pushback on these decoy systems, they do seem to be unrolling persistently and slowly becoming the norm.[5] It is important to remember that while data may be those that are pursued, those data reference individuals and can be used to assert forms of surveillant control over them, to modulate behavior, to discipline, and to punish. As Grégoire Chamayou (2012) argues, the pastoral power theorized by Michel Foucault was always coupled with the dehumanizing power of manhunts, which sought to capture or expel those marked as out of place, be they deviant, poor, or other. Chamayou writes, "Whereas pastoral power guides and accompanies a multiplicity in movement, cynegetic power extends itself, on the basis of a territory of accumulation, over a space of capture" (Chamayou 2012, 16). The decoy trash bins, phone booths, and airplanes each overlay a grid over territory and establish a field for the hunt—of potential consumers or suspected criminals. Following Chamayou, though, we can say that these decoys also reinforce a set of political prerogatives: whether toward a digital enclosure that reduces technological possibility to commercial interests (Andrejevic 2007) or toward the assertion of police and state domination (Wall 2013). The hunt for data becomes itself a kind of violence against the possible.

Conclusion

This article has argued that deceptive communication systems are hidden articulations of normal technological orders. They are polyvalent and polyvocal; they are oriented toward surveillance and control, especially in their hidden functions; and they are commonplace and often legal. The examples reviewed here range from the seemingly pedestrian installation of untrustworthy hotel and workplace thermostats, to widespread and troubling cases of surveillance of computer activity, to the apparently extreme collection of mobile phone metadata by private companies and law enforcement agencies. If one approaches these examples not as isolated cases but instead as significant indicators of technological trends more broadly, then responses or correctives should be more encompassing.

If deception in itself is not the primary problem with such systems, or with communication more broadly, then transparency alone cannot be the solution. A call for greater transparency could be akin to quests to eradicate noise from transmission systems in the belief that pure communication could be approximated and that it could produce rational responses that curtailed abuse. In short, calls for transparency may unwittingly ignore the ritualistic dimensions of technologies and the inescapable politics of all communicative acts. As troubling as institutional opacity might be, more fundamental problems revealed by deceptive systems are imbalances in power and widespread acquiescence to corporate and state efforts to control individuals, groups, and their data. The issues are about rights claimed by institutions through technological means without significant contestation by publics, which is a dynamic that effectively legitimizes such control practices, along with corporate and state ownership of data collected through them. Therefore, the most pressing imperative is not necessarily to choose different systems, but instead to change the field upon which they are cast.

Notes

1. It should also be noted that transparency is a value-laden concept that in practice often privileges the relatively white and affluent while designating others as opaque and therefore dangerous (Hall 2015).
2. As banal as thermostats and climate control systems might appear, those without access to them face greater health risks, especially in extreme weather situations (Rogot et al. 1992; Poulter 2012), and reliance on them could contribute greatly to costly energy expenditures and destructive climate change (Oatman 2015; Rosenthal and Lehren 2012).
3. As evidence that not everyone is as compliant, a number of websites offer suggestions for hacking standard

thermostats to afford a wider range of user discretion over temperature settings (e.g., Henry 2013).
4. In 2015, the U.S. Department of Justice changed its policy to require federal agents to obtain a warrant before deploying Stingray devices, but this policy change does not apply to local or state police forces (Fandos 2015).
5. This trend can be witnessed with related applications like Apple's iBeacon, which allows businesses to identify, track, and advertise to potential customers through their mobile phones (Ranger 2014).

Acknowledgments

The author would like to thank Bill Staples and the participants of the 2015 "States of Surveillance" symposium at the University of Kansas for their insightful suggestions on an earlier draft of this article.

References

Aas, K. F. 2006. 'The body does not lie': Identity, risk and trust in technoculture. *Crime, Media, Culture* 2 (2):143–58.

Akrich, M. 1992. The de-scription of technological objects. In *Shaping technology/Building society: Studies in sociotechnical change*, ed. W. E. Bijker, and John Law, 205–24. Cambridge, MA: The MIT Press.

Alder, G. S., M. L. Ambrose, and T. W. Noel. 2006. The effect of formal advance notice and justification on Internet monitoring fairness: Much about nothing? *Journal of Leadership & Organizational Studies* 13 (1):93–107.

American Civil Liberties Union. 2015. Stingray tracking devices: Who's got them? http://www.aclu.org/map/stingray-tracking-devices-whos-got-them (accessed February 16, 2016).

Andrejevic, M. 2007. *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University Press of Kansas.

Andrejevic, M. 2013. *Infoglut: How too much information is changing the way we think and know*. New York, NY: Routledge.

Arabe, K. C. 2003. "Dummy" thermostats cool down tempers, not temperatures. *ThomasNet News*, April 11. http://news.thomasnet.com/imt/2003/04/11/dummy_thermosta (accessed August 30, 2015).

Arditi, D. 2013. iTunes: Breaking barriers and building walls. *Popular Music and Society* 37 (4):408–24.

Ball, K. 2010. Workplace surveillance: An overview. *Labor History* 51 (1):87–106.

Baral, S. 2012. EcoInsight thermostats reduce Hilton Hotels energy usage by 35%. *Greener Ideal*, November 19. http://www.greenerideal.com/business/1119-ecoinsight-thermostats-save-hilton-hotels-energy (accessed September 5, 2015).

Baraniuk, C. 2015. Press me! The buttons that lie to you. *BBC.com*, April 17. http://www.bbc.com/future/story/20150415-the-buttons-that-do-nothing (accessed August 30, 2015).

Barrett, D. 2014. Americans' cellphones targeted in secret U.S. Spy program. *Wall Street Journal*, November 13. http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533 (accessed September 5, 2015).

Bowker, G. C., and S. L. Star. 1999. *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

boyd, D., and K. Crawford. 2012. Critical questions for big data. *Information, Communication & Society* 15 (5):662–79.

Browne, S. 2015. *Dark matters: On the surveillance of blackness*. Durham, NC: Duke University Press.

Brucato, B. 2015. Policing made visible: Mobile technologies and the importance of point of view. *Surveillance & Society* 13 (3/4):455–73.

Brunton, F., and H. Nissenbaum. 2011. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday* 16 (5). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955 (accessed July 19, 2011).

Campbell-Dollaghan, K. 2013. Brave new garbage: London's trash cans track you using your smartphone. *Gizmodo*, August 9. http://gizmodo.com/brave-new-garbage-londons-trash-cans-track-you-using-1071610114 (accessed September 5, 2015).

Carey, J. W. 1992. *Communication as culture: Essays on media and society*. New York, NY: Routledge.

CBS/AP. 2013. U.K. bars trash cans from tracking people with Wi-Fi. August 12. http://www.cbsnews.com/news/uk-bars-trash-cans-from-tracking-people-with-wi-fi (accessed September 5, 2015).

Chamayou, G. 2012. *Manhunts: A philosophical history*, trans. S. Rendall. Princeton, NJ: Princeton University Press.

Cobley, P. 2001. *The Routledge companion to semiotics and linguistics*. New York, NY: Routledge.

Cohen, J. E. 2008a. Privacy, visibility, transparency, and exposure. *University of Chicago Law Review* 75 (1):181–201.

Cohen, J. E. 2012. *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven, CT: Yale University Press.

Cohen, N. S. 2008b. The valorization of surveillance: Towards a political economy of facebook. *Democratic Communiqué* 22 (1):5–22.

Cole, S. A., and H. N. Pontell. 2006. "Don't be low hanging fruit": Identity theft as moral panic. In *Surveillance and security: Technological politics and power in everyday life*, ed. T. Monahan, 125–47. New York, NY: Routledge.

Couldry, N. 2003. *Media rituals: A critical approach*. New York, NY: Routledge.

CresendoCrook. 2015. TIL: Honeywell thermostats have a function that allows hotels/landlords to misrepresent room temperature up to +/− 3 degrees. Reddit.com. http://www.reddit.com/r/todayilearned/comments/2ru820/til_honeywell_thermostats_have_a_function_that/ (accessed September 5, 2015).

Cushing, T. 2013. LG smart TV caught collecting data on files stored on connected USB drives. *Techdirt*, November 20. http://www.techdirt.com/articles/20131119/06503625288/lg-smart-tv-caught-collecting-data-files-stored-connected-usb-drives.shtml (accessed September 5, 2015).

Doctorow, C. 2014. US marshals raid Florida cops to prevent release of records of "stingray" surveillance. BoingBoing.net, June 4. https://boingboing.net/2014/06/04/us-marshals-raid-florida-cops.html (accessed September 5, 2015).

Dwoskin, E. 2014. New York city shuts down unauthorized sensors. *Wall Street Journal*, October 7. http://blogs.wsj.com/digits/2014/10/07/new-york-city-shuts-down-unauthorized-sensors (accessed September 5, 2015).

Fandos, N. 2015. Justice Dept. to require warrants for some cellphone tracking. *New York Times*, September 3. http://www.

nytimes.com/2015/09/04/us/politics/justice-dept-to-require-warrants-for-some-cellphone-tracking.html (accessed September 5, 2015).

Farivar, C. 2014. Cities scramble to upgrade "stingray" tracking as end of 2G network looms. *Ars Technica*, September 1. http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms (accessed August 30, 2015).

Fitchett, J., and M. Lim. 2008. Consumer experiences in the "house of the future": An enquiry into surveillance-based consumer research techniques. *Consumption Markets & Culture* 11 (2):137–49.

Gates, K., and S. Magnet. 2007. Communication research and the study of surveillance. *The Communication Review* 10 (4):277–93.

Gilliom, J., and T. Monahan. 2013. *SuperVision: An introduction to the surveillance society*. Chicago, IL: University of Chicago Press.

Gillum, J., E. Sullivan, and E. Tucker. 2015. FBI behind mysterious fleet of aircraft conducting surveillance over US cities. June 2. *Star Tribune*. http://www.startribune.com/fbi-behind-mysterious-surveillance-aircraft-over-us-cities/305793361 (accessed September 5, 2015).

Gregg, M. 2013. Spousebusting: Intimacy, adultery, and surveillance technology. *Surveillance & Society* 11 (3):301–10.

Grochmal, G. 2013. Energy management systems for hotel guest rooms. *EcoGreenHotel*, October 24. http://www.ecogreenhotel.com/blog/energy-management-systems-for-hotel-guest-rooms (accessed August 30, 2015).

Haggerty, K. D., and R. V. Ericson. 2000. The surveillant assemblage. *British Journal of Sociology* 51 (4):605–22.

Hall, R. 2015. *The transparent traveler: The performance and culture of airport security*. Durham, NC: Duke University Press.

Han, B.-C. 2015. *The transparency society*. Stanford, CA: Stanford University Press.

Handley, J. 2014. Slip of an officer's tongue suggests police are monitoring #BlackLivesMatter protesters' cell phones. *In These Times*, December 19. http://inthesetimes.com/article/17476/a_slip_of_an_officers_tongue_suggests_police_are_monitoring_ferguson_protes (accessed August 30, 2015).

Harris, S. 2015. Your Samsung SmartTV Is spying on you, basically. *The Daily Beast*, February 5. http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html (accessed August 30).

Hasek, G. 2011. Energy management system suppliers build on proven, money-saving technologies. *Green Lodging News*, February 7. http://www.greenlodgingnews.com/energy-management-system-suppliers-build-on-proven (accessed September 5, 2015).

Henry, A. 2013. Override your hotel room thermostat and set it as hot or cold you like. Lifehacker.com, November 12. http://lifehacker.com/override-your-hotel-room-thermostat-and-set-it-as-hot-o-1462595059 (accessed September 5, 2015).

Hoffelder, N. 2014. Adobe is spying on users, collecting data on their eBook libraries. *The Digital Reader*, October 6. http://the-digital-reader.com/2014/10/06/adobe-spying-users-collecting-data-ebook-libraries (accessed September 5, 2015).

Honeywell. 2015. ecoMODE. Inncom.com. http://www.inncom.com/catalog/item/ecomode (accessed September 5, 2015).

InterGuard. 2015. InterGuard: Employee monitoring software. http://www.interguardsoftware.com (accessed September 5, 2015).

Introna, L. D. 2000. Workplace surveillance, privacy and distributive justice. *Computers and Society* 30 (4):33–39.

Kiser, A. I. T., T. Porter, and D. Vequist. 2010. Employee monitoring and ethics: Can they co-exist? *International Journal of Digital Literacy and Digital Competence* 1 (3):30–45.

Kiss, S., and V. Mosco. 2005. Negotiating electronic surveillance in the workplace: A study of collective agreements in Canada. *Canadian Journal of Communication* 30 (4):549–64.

Langer, E. J. 1975. The illusion of control. *Journal of Personality and Social Psychology* 32 (2):311–28.

Leonardi, P. M. 2012. *Car crashes without cars: Lessons about simulation technology and organizational change from automotive design*. Cambridge, MA: MIT Press.

Lyon, D. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1 (2):1–13.

Lyon, D. 2015. *Surveillance after Snowden*. Malden, MA: Polity.

Maass, D. 2014. ComputerCOP: The dubious 'Internet safety software' that hundreds of police agencies have distributed to families. Electronic Frontier Foundation, October 1. http://www.eff.org/deeplinks/2014/09/computercop-dangerous-internet-safety-software-hundreds-police-agencies (accessed September 5, 2015).

Marx, G. T., and V. Steeves. 2010. From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society* 7 (3/4):192–230.

Mason, C., and S. Magnet. 2012. Surveillance studies and violence against women. *Surveillance & Society* 10 (2):105–18.

Mayer-Schönberger, V., and K. Cukier. 2013. *Big data: A revolution that will transform how we live, work, and think*. Boston, MA: Houghton Mifflin Harcourt.

Monahan, T. 2009. Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology* 13 (2):155–76.

Monahan, T. 2010. *Surveillance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.

Monahan, T. 2015. The right to hide? Anti-surveillance camouflage and the aestheticization of resistance. *Communication and Critical/Cultural Studies* 12 (2):159–78.

Morozov, E. 2013. Is smart making us dumb? *Wall Street Journal*, February 23. http://www.wsj.com/articles/SB10001424127887324503204578318462215991802 (accessed June 19, 2015).

Mosco, V. 2014. *To the cloud: Big data in a turbulent world*. New York, NY: Paradigm.

Mumby, D. K. 2005. Theorizing resistance in organization studies: A dialectical approach. *Management Communication Quarterly* 19 (1):19–44.

Murakami Wood, D., and K. Ball. 2013. Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory* 13 (1):47–67.

My Team Monitor. 2013a. Employer interface video. http://www.myteammonitor.com (accessed September 5, 2015).

My Team Monitor. 2013b. Introductory video. http://www.myteammonitor.com (accessed September 5, 2015).

Oatman, M. 2015. Chilling effect: How air conditioning is making us hotter. *Mother Jones*, September/October, 66–67.

Oudshoorn, N. 1999. On masculinities, technologies, and pain: The testing of male contraceptives in the clinic and the media. *Science, Technology, and Human Values* 24 (2):265–89.

Owano, N. 2013. SideWays eye-tracking system shown at Paris conference (w/ video). Phys.org, May 1. http://phys.org/

news/2013-05-sideways-eye-tracking-shown-paris-conference.html (accessed August 16, 2015).

Packer, J., and S. B. C. Wiley, eds. 2012. *Communication matters: Materialist approaches to media, mobility and networks*. New York, NY: Routledge.

Pasquale, F. 2015. *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Pelican Wireless Systems. 2011. Renaissance ClubSport hotel reduces HVAC energy costs by 35%. Pelican Wireless Systems. http://www.pelicanwireless.com/case-studies/clubsport-renaissance-hotel-reduces-hvac-energy-costs-by-35 (accessed September 5, 2015).

Peters, J. D. 1999. *Speaking into the air: A history of the idea of communication*. Chicago, IL: University of Chicago Press.

Pfaffenberger, B. 1992. Technological dramas. *Science, Technology, and Human Values* 17 (3):282–312.

Plumer, B. 2015. Volkswagen's appalling clean diesel scandal, explained. *Vox.com*, September 23. http://www.vox.com/2015/9/21/9365667/volkswagen-clean-diesel-recall-passenger-cars (accessed October 12, 2015).

Poulter, S. 2012. 24,000 'died because of cold homes' last winter: Fears grow that figure could be higher this year because of spiralling bills. *The Daily Mail*, November 29. http://www.dailymail.co.uk/news/article-2240716/24-000-died-cold-homes-winter-Fears-grow-figure-higher-year-spiralling-bills.html (accessed August 31, 2015).

Quintin, C. 2014. What we can learn from the Adobe e-reader mess. Electronic Frontier Foundation, October 31. http://www.eff.org/deeplinks/2014/10/what-we-can-learn-adobe-e-reader-mess (accessed September 5, 2015).

Ranger, S. 2014. What is Apple iBeacon? Here's what you need to know. ZDNet.com, June 10. http://www.zdnet.com/article/what-is-apple-ibeacon-heres-what-you-need-to-know (accessed September 5, 2015).

Regan, P. M. 2003. Privacy and commercial use of personal data: Policy developments in the United States. *Journal of Contingencies and Crisis Management* 11 (1):12–18.

Rogot, E., P. D. Sorlie, and E. Backlund. 1992. Air-conditioning and mortality in hot weather. *American Journal of Epidemiology* 136 (1):106–16.

Rosenthal, E., and A. W. Lehren. 2012. Relief in every window, but global worry too. *New York Times*. http://www.nytimes.com/2012/06/21/world/asia/global-demand-for-air-conditioning-forces-tough-environmental-choices.html (accessed August 31, 2015).

RT.com. 2014. *Mysterious unidentified spying cell towers found across*. Washington, DC: RT.com. http://www.rt.com/usa/189116-washington-dc-spying-phone (accessed September 5, 2015).

Sandberg, J. 2003. Employees only think they control thermostat. *Wall Street Journal*, January 15. http://www.wsj.com/articles/SB1042577628591401304 (accessed August 30, 2015).

Schneider Electric. 2010. Cassia energy management system [promotional brochure]. May. http://www.schneider-electric.com/solutions/au/en/med/4664417/application/pdf/1056-cassia-6pg-promotional-brochure.pdf (accessed September 5, 2015).

Schneider Electric. 2015. Cassia™ in-room energy management system. Schneider Electric USA. http://www.schneider-electric.us/en/product-range/61302-cassia–in-room-energy-management-system (accessed August 30, 2015).

Schüll, N. D. 2012. *Addiction by design: Machine gambling in Las Vegas*. Princeton, NJ: Princeton University Press.

Sharma, S. 2014. *In the meantime: Temporality and cultural politics*. Durham, NC: Duke University Press.

Slack, J. D., and J. M. Wise. 2005. *Culture and technology: A primer*. New York, NY: Peter Lang.

Spitzberg, B. H., and W. R. Cupach. 2011a. *The dark side of interpersonal communication*, 2nd ed. New York, NY: Routledge.

Spitzberg, B. H., and W. R. Cupach. 2011b. Disentangling the dark side of interpersonal communication. In *The dark side of interpersonal communication*, ed. B. H. Spitzberg and W. R. Cupach, 3–28. New York, NY: Routledge.

Staples, W. G. 2014. *Everyday surveillance: Vigilance and visibility in postmodern life*. 2nd ed. Lanham, MD: Rowman & Littlefield.

Strohmeyer, R. 2011. How to monitor your employees' PCs without going too far. *PC World*, March 22. http://www.pcworld.com/article/222169/how_to_monitor_your_employees_without_going_too_far.html (accessed September 5, 2015).

Taylor, F. W. 1911. *The principles of scientific management*. New York, NY: Harper & Brothers.

TeenSafe. 2015. TeenSafe: iPhone tracker and cell phone monitoring. http://www.teensafe.com (accessed August 16, 2015).

Tobii. 2015. Advertising research and eye tracking. Tobii.com, May 1. http://www.tobii.com/eye-tracking-research/global/research/advertising-research (accessed August 16, 2015).

Wall, T. 2013. Unmanning the police manhunt: Vertical security as pacification. *Socialist Studies* 9 (2):32–56.

Whitson, J. R., and K. D. Haggerty. 2008. Identity theft and the care of the virtual self. *Economy and Society* 37 (4):572–94.

Winner, L. 1980. Do artifacts have politics? *Daedalus* 109:121–36.

Winner, L. 1986. *The whale and the reactor: A search for limits in an age of high technology*. Chicago, IL: University of Chicago Press.

Woolley, J., M. Pritoni, M. Modera, and T. Peffer. 2014. Why occupancy-responsive adaptive thermostats do not always save—and the limits for when they should. Paper read at ACEEE Summer Study on Energy Efficiency in Buildings. aceee.org/files/proceedings/2014/data/papers/3-490.pdf (accessed September 5, 2015).

Wrege, C. D., and A. G. Perroni. 1974. Taylor's pig-tale: A historical analysis of Frederick W. Taylor's pig-iron experiments. *Academy of Management Journal* 17 (1):6–27.

Zetter, K. 2014. U.S. Marshals seize cops' spying records to keep them from the ACLU. Wired.com, June 3. http://www.wired.com/2014/06/feds-seize-stingray-documents (accessed September 5, 2015).