First Monday, Volume 20, Number 7 - 6 July 2015

PEER-REVIEWED JOURNAL ON THE INTERNET

The spectrum of control: A social theory of the smart city

by Jathan Sadowski and Frank Pasquale

Abstract

There is a certain allure to the idea that cities allow a person to both feel at home and like a stranger in the same place. That one can know the streets and shops, avenues and alleys, while also going days without being recognized. But as elites fill cities with “smart” technologies — turning them into platforms for the “Internet of Things” (IoT): sensors and computation embedded within physical objects that then connect, communicate, and/or transmit information with or between each other through the Internet — there is little escape from a seamless web of surveillance and power. This paper will outline a social theory of the “smart city” by developing our Deleuzian concept of the “spectrum of control.” We present two illustrative examples: biometric surveillance as a form of monitoring, and automated policing as a particularly brutal and exacting form of manipulation. We conclude by offering normative guidelines for governance of the pervasive surveillance and control mechanisms that constitute an emerging critical infrastructure of the “smart city.”

Contents

I. Introduction

There is a certain allure to the idea that cities allow a person to both feel at home and like a stranger in the same place. That one can know the streets and shops, avenues and alleys, while also going days without being recognized. But as government and corporate actors, often in close partnership with each other, fill cities with “smart” [1] technologies — turning them into platforms for the “Internet of Things” (IoT): sensors and computation embedded within physical objects that then connect, communicate, and/or transmit information with or between each other through the Internet — there is little escape from a seamless web of surveillance (*cf.*, Hollands, 2008; Townsend, 2014; Neirotti, *et al.*, 2014). Soon, for example, shoppers and viewers will be as “known” by a store or gallery as they are able to know it (Arnsdorf, 2010). Facial recognition software, or smartphone emanations, can project your identity, likely spending habits, and reputation: shoplifter or big spender, “Mortgage Woes” or “Boomer Barons” (to use actual categories from marketers) (Castle Press, 2010).

“Big data” is the new currency of commerce, but like money, some have far better terms of access to it than others. In finance, the average borrower must turn over detailed, personal records to receive a loan; the bank is under no parallel obligation, though, to explain its own internal decision-making in nearly as much detail (Pasquale, 2015). The same dynamics are emerging in the IoT: powerful entities centripetally attracting more data from their users, but denying access to users and regulators, even when very troubling data uses and breaches occur. It no longer makes sense to think of “the Internet” as a thing that one accesses via a computer. Not when the city itself is reimagined and reconstructed as a platform for and node within networked information-communication technologies (ICT).

Wired's flagship article on the IoT asks, "Have you ever lost an object in your house and dreamed that you could just type a search for it, as you would for a wayward document on your hard drive?" (Wasik, 2013). Well you can now, we are assured, thanks to a startup called StickNFind Technologies that sells cheap, small, "sticker" sensors. Lose a child at the mall? "Smart fashion" RFID tags will keep him or her plugged into the network and tracked at all times. And why stop with kids when making sensor-laden sartorial choices? Before long your car, house, appliances, and every other part of your environment will be engaging in a constant stream of networked communication with each other. Taken at the urban scale, the city becomes a cocoon of connectivity that engulfs us — or, alternatively, it becomes a web that ensnares us — as smart technologies are integrated into our everyday lives. These technologies are billed as modes of finding, of wayfaring. They are technologies of search (when we apply them) and technologies of reputation (when used to evaluate us) (Pasquale, 2015). They map, categorize, and classify — and what could be more innocuous than mere information?

Calculating the costs and benefits of the innovation is a Sisyphean, and deeply ideological, task. Who knows what sinister or spectacular applications may emerge? Scenario analysis and planning could be a valuable alternative to cost-benefit studies (Verchick, 2010): these methods acknowledge the incommensurability of the gains in convenience, and losses of privacy, portended by the IoT. But corporate *and* government discourse on IoT has tended to marginalize the most important *negative* scenario analyses, downplaying them as paranoid projections. Technocrats distort policy evaluations of pervasive surveillance and control in urban environments. Moreover, their normative tools of evaluation, focusing on consumer and citizen "consent" to surveillance, are manipulable enough to embrace even the most disturbing technologies of control — such as drone-driven crowd control directed at protesters, or automobile loan technology that disables cars mere minutes after a payment is late — as expressions of democratic will and market rationality.

Technocrats' convenient blindness to the most worrisome aspects of the "smart city" invites a more balanced theoretical response. We propose one such response that lays out the characteristics and consequences of a dominant socio-political logic that courses throughout and ties together many of the various practices and ideologies related to "smart cities." We begin by providing a contextual overview of the "smart city," building from the burgeoning analytical work on the topic. This leads into a critical introduction to the ideology of the "smart city," focusing on the stated aspirations of some of its most notable corporate, governmental, and academic exponents. We then offer a Deleuzian alternative, outlining a social theory of the "smart city" in *service to capital* as a form of control (rather than emancipation) of its subject-citizens. Next, we present two illustrative examples along the resulting spectrum of control: biometric surveillance as a form of monitoring, and automated policing as a particularly brutal and exacting form of manipulation. Our penultimate section makes explicit the stakes of the deep integration of person–machine — city in our "post-digital-dualist era" (Jurgenson, 2012). And we end by offering some normative guidelines for governance of the pervasive surveillance and control mechanisms that constitute the emerging critical infrastructure of the "smart city."

II. What is a smart city?

Globally — in terms of market valuation, expendable capital, technological development, and transformative influence — the smart city movement has been growing at a rapid pace. A 2013 report, released by the United Kingdom's Department for Business, Innovation and Skills, estimated that "the global market for smart city solutions and the additional services required to deploy them [will] be $408 billion by 2020." Linked to this growth is the exponential expansion of the IoT. According to commonly cited numbers from telecommunications giant Cisco, one of the major industries involved in the IoT and smart cities, billions of things are already connected — "over 12.5 billion devices in 2010 alone." And they predict, "Some 25 billion devices will be connected by 2015, and 50 billion by 2020." [2] Less conservative estimates place the smart city market into the trillion(s) of dollars over the next five to ten years, with the IoT market being worth even more. Case in point, IBM recently announced it would be investing US$3 billion over the next four years in creating a new IoT unit (Reuters, 2015) — an investment that will surely boost IBM's already lucrative, multi-billion dollar "Smarter Planet" initiative. As an urban planning and governance movement, a lot of effort is expended on pushing and pulling "smartness" — the major corporate players work hard to push smartness as an ideal and to pull city leaders and investors into the smartness orbit. These corporations did not just stumble upon an existing market for which they could fill the needs. They, rather, have worked hard to create this market and to shape it in certain ways.

Yet, with this massive growth and capital investment, the label "smart city" is nebulous. There's not a single definition that can be called up and applied anytime the label is invoked (Hollands, 2008). This ambiguity does a lot of work for smart city proponents and purveyors. The label is treated like a floating signifier that can change referents whenever needed. Allowing for a flexible, dynamic space in which to plug a variety of products, practices, and policies. Giving them discursive cover in case they need to distance themselves if something goes wrong or doesn't deliver on a promise.

One important and constant characteristic of these different visions, however, is that they aim to evoke positive change and innovation — at least as the proponents see it — via digital ICT; essentially, building an IoT at the city-scale by installing networked objects throughout the urban environment (and even human bodies) for a wide range of different purposes. The typical examples used to illustrate an IoT-filled world are consumer products — like the ever-present smart fridge that tells the store when you need milk. But, Bruce Sterling argues, this is a "fairy tale," instead "the genuine Internet of Things wants to invade that refrigerator, measure it, instrument it, monitor any interactions with it; it would cheerfully give away a fridge at cost" [3]. Restricting our focus to the consumer devices poses a red herring that keeps our attention at the surface level, halting analyses that should go beyond the alternating currents of absurd farce and gee whiz excitement. "These grand, world-scale [corporate] alliances did not form in order to sell the reader a smart refrigerator. Most of them would really like the reader to dwell in a 'Smart City' where they supply the 'smartness' on their own terms — and they're not much concerned about the reader's consent as a citizen" [4]. The smart city is not just a linearly scaled version of the smart home where all of our personal devices and domestic appliance are networked, automated, and good communicators. It is fundamentally about infrastructural and civic applications — the kind of things that constitute the techno-political ordering of society — and it is about the data and control those applications generate. To be sure, not all "smart cities" are implemented in the same way; we see three main types.

First, by far the most common 'actually existing' smart cities are those that are *retrofitted and renovated* with upgrades that transition current cities from dumb to smart. Many estimates place the number of cities and towns with smart initiatives into the tens or hundreds of thousands around the world. In these cases, "the smart city is assembled piecemeal, integrated awkwardly into existing configurations of urban governance and the built environment" [5]. Typically the underlying motivations are political economic, the result of an increasingly entrepreneurial form of urban governance that seeks to make the city into a center of (regionally or globally) competitive economic growth and activity (Harvey, 1989). Getting smart is the handy panacea for overcoming austerity, managing the urban system, and becoming an attractive place for capital to flow into — all by using "networked infrastructures to improve economic and political efficiency and enable social, cultural and urban development" [6]. Hence, smart initiatives promise to provide city leaders with the means necessary for achieving their entrepreneurial ends.

Second, there is the 'shock therapy' method — or, what we might call *smart shock* — wherein a city undergoes a quick, large-scale integration of 'smart' ideals, technologies, and policies into an existing landscape. There are not as yet any cities that have experienced a full shock, but rather there are examples where the smart city transition has occurred to a greater degree and at a more rapid pace than the typical retrofits. Perhaps the best example is the Intelligent Operations Center built in 2010 by IBM for the city of Rio de Janeiro, which "draws together data streams from thirty agencies, including traffic and public transport, municipal and utility services, emergency services, weather feeds, and information sent in by employees and the public via phone, Internet and radio, into a single data analytics centre" [7]. With this NASA-esque control room, the city of Rio is turned into a system for optimization and securitization. Different parts of city life can be scrutinized and managed at a more exacting level, thus amplifying the already existing practices of militaristic urban control (Wacquant, 2008). IBM and other technology corporations have created similar data centers elsewhere for single agencies like police departments, but none have yet reached the magnitude of Rio's Intelligent Operations Center. Though, there is plenty of indication that Rio foreshadows the type of systems we can expect to see being rapidly built and deployed in other cities.

Third, the idealistic models for the smart city are the *built from scratch* projects that are being constructed where nothing existed before. A canonical case is New Songdo in South Korea, which serves as a global test-bed (Halpern, *et al.*, 2013) and urban laboratory (Gieryn, 2006) for implementing large-scale smart systems in the wild. At a cost of approximately US$40 billion, Songdo's corporate and government backers hope to make it the world's first fully smart city. As Christine Rosen (2012) remarks, "Songdo claims intelligence not from its inhabitants, but from the millions of wireless sensors and microcomputers embedded in surfaces and objects throughout the metropolis." This type of implementation represents a zone of futurity. That is, a window into a grand, but plausibly potential, urban future. Furthermore, this type also reveals striking historical similarities that exists between the smart city ideology and the ideology of twentieth century high-modernist architecture. Consider that Brazil's federal capital of Brasília — a monument to the high-modernism ideals of technocratic administrative ordering — was built, in only 41 months (1956–1960), by clearing out a plot of land in the Amazon rainforest (Scott, 1998). "Point by point," writes Adam Greenfield [8], "whether they do so out of ignorance, ahistoricity, heedlessness or hubris, the designers of Songdo and Masdar and PlanIT Valley [other canonical smart cities] recapitulate the overspecification, overweening scientism and ponderous authoritarian pomposity of Chandigarh and Brasília, right down to the grand ceremonial axes."

Even with this plurality of methods and motivations, we believe it is possible *and necessary* to begin parsing out the underlying socio-political logics that these smart city initiatives hold in common. As we have shown, there's no sign that the smart city is slowing down. The ideals and practices of the movement — in the various styles they are implemented — continue to colonize the urban landscape and political imaginations of city leaders. Given the constraints of this paper, our overview is only meant to set the stage for the critical social theory at the heart of this paper. For a more exhaustive genealogical analysis of the dominant discourses and ideologies that are driving these sociotechnical systems and policies — specifically those emanating from the major corporate actors of IBM, Cisco, and Siemens — we point the reader to Adam Greenfield's thorough pamphlet, *Against the smart city* (2013). What's more, we should be clear that our generalized use of "smart city" in the rest of the article is meant to be a shorthand for technologies and techniques that align with both the practices and ideologies of the "smart city" label — no matter what their scale or style of implementation. We don't intend to homogenize or flatten out the differences in what the "smart city" means for different cities, policy-makers, and corporations. Rather, our hope is to draw attention to the ways in which seemingly disparate technologies and techniques have origins in and reproduce common socio-political logics — and we will do this by discussing specific initiatives. But first, the next section introduces the ideologies — updating and adding depth to Greenfield's own study — that are embedded within and enacted by smart city initiatives.

III. The ideology of the smart city

In more formal spaces of policy advocacy, a stark meliorism informs a Whiggish imaginary of technological progress via the IoT. In a widely cited article for *Foreign Affairs*, two chief executives for Cisco trumpeted the benefits of applying the "Internet of Everything" to nearly all aspects of city infrastructure and governance (Chambers and Elfrink, 2014). They promised "intelligent and efficient stewardship of growing cities" to reduce "traffic, parking congestion, pollution, energy consumption, and crime." Who could be against such a program? The only cost, the executives assure readers, would be a slight reorientation in governance and IT procurement strategies. First, "the world must rethink IT investments" by "moving away from purchasing isolated services and instead focusing on end-to-end solutions that are integrated across disparate or siloed systems." Second, "hyper collaborative partnerships between the public and private sectors" with strict "adherence to deadlines" is essential. As one of their principles for making smart cities the global "norm" proclaims, "the world can't be afraid of embracing technology in new ways. This means rethinking the contract with citizens and the services IT firms and governments provide them" (Chamber and Elfrink, 2014).

The shift in political language — wherein the social contract is replaced by the corporate contract — is subtle, but critical for understanding the politics smuggled into the technocratic agenda of smart cities (*cf.*, Sadowski and Selinger, 2014). This explains why the six principles they propose are all based on admonishing "city leaders" for not valorizing (enough) the products and services offered by the ICT sector. Like savvy businessmen, the authors recognize the asymmetry of public-private partnerships in an era of neoliberalism. When top managers at firms earn many multiples of top civil servants, the latter readily allow the private sphere to reshape the public sphere in its own image. Corporations can afford a phalanx of economists, designers, attorneys, and public relations specialists, all skilled in presenting one possible future for the city as a technocratic *pensée unique*. Indeed, other than the corporate model, "there exist no large-scale alternative smart city models, partly because most cities have generally embraced a pro-business and entrepreneurial governance model of urban development" [9].

Of course, Cisco has a commercial interest here: designing, manufacturing, and installing the hardware for these networks is Cisco's lifeblood, and future profit margins may depend on the firm's ability to craft seductive narratives of 'smartness.' But numerous municipal leaders and non-profit foundations have jumped on the bandwagon, as well. There are material motivations here, too, as politico-economic analyses of revolving door employment patterns between private, public, and "third" sector concerns reveal. When civil servants can easily multiply their pay by moving from government to corporate offices, as long as they are pliable and cooperative, few have an incentive to ask hard questions (Carpenter and Moss, 2013). The boundaries between public office and private consulting are porous.

Just as important as material motives and career ambition, the *narrative* of the smart city, as an interpretation of technological systems, rationalizes these urban transformations (Söderström, *et al.*, 2014). In a commentary on smart cities research, geographer Rob Kitchin argues that it is problematic the way in which "much of the writing and rhetoric about smart cities" — whether stemming from business, academia, or government — "seeks to appear non-ideological, commonsensical and pragmatic" [10]. This is an outgrowth of a technocratic neoliberal ideology, and a broader political economic imaginary of stable extraction of profits and taxes. Advocates of the smart city style themselves as hard-headed problem solvers who transcend the zero-sum politics that cause other to become embroiled in gridlocked conflict. Yet, they all too often slip into the attitude memorably parodied by Clifford Geertz as "I have a social philosophy; you have political opinions; he has an ideology" [11]. Here the "I" might be smart city contractors; the "you," city leaders; and "he" the various interest groups raising deeper concerns about the implementation of mass surveillance, data processing, and control. Take, for instance, a speech by Samuel Palmisano (2010), then the Chairman, President, and CEO of IBM, in which he asserted, "Building a smarter planet is realistic precisely because it is so refreshingly non-ideological." However, as Geertz advises, the deployment of the term ideology is one of the most ideologized practices of modern rhetoric, a way of concealing the more contestable values and assumptions driving those dismissing their opponents as ideological. In this paper, we do not use the term ideology as an *a priori* accusation, but rather in its descriptive capacity — and somewhat ironically since many technologists and neoliberals alike expend so much energy claiming that their practices are the results of a value-free, Progress-driven, extra-human force (*e.g.*, technology and markets).

To better understand the invariably political character of the smart city, consider a logical extension of some current smart city thinking, proposed as a thought experiment by philosopher and legal theorist Lawrence Solum. Singapore has "smart intersections that var[y] their red/green cycles according to traffic" (Baum, 2001), and one can imagine far more elaborate methods of controlling the flow of automobiles. Solum posits the development of an "Artificially Intelligent Traffic Authority (AITA)," which could "adapt itself to changes in driver behavior and traffic flow" [12]. The system would be designed to "introduce random variations and run controlled experiments to evaluate the effects of various combinations on traffic pattern" [13], recalling Jim Manzi's (2012) recommendations for far more experimentation in public policy. But the system would not be very forgiving of *individual* experimentation with, say, violating its rules. Rather, as imagined by Solum, "[v]iolations would be detected by an elaborate system of electronic surveillance" and offenders would be "identified and immediately would be removed from traffic by a system of cranes located at key intersections" [14].

Solum uses this example to break down the usual distinctions between human and artificial meaning in law, rather than as a policy proposal for the future of traffic. The scenario is just as useful to flag the inevitably *legal* and *political* aspects of automated law enforcement, even in an area as seemingly technical as traffic. Would the cranes posited in Solum's hypothetical surgically remove protesters, like the Ferguson marchers, who blocked highways (Harcourt, 2012)? Would anyone with an expired license or tags be plucked away as well — in a vision already half-realized by subprime lenders who stop cars remotely as soon as a payment is late (Sadowski and Pasquale, 2014)?

The problem for smart city advocates is one of overcoming several tensions, if not outright contradictions, in their ideal-type of corporatized governance. Who is ultimately in charge of "hyper collaborative partnerships between the public and private sectors?" What are the penalties when, say, deadlines are not met? Who imposes them? What are the problems that the smart city will use "end-to-end solutions" to solve? How will the imposition of such "solutions" be sequenced?

To take some obvious examples: should new forms of surveillance focus first on drug busts, or evidence of white-collar crime, or unfair labor practices by employers? Wage theft is a massive problem, but rarely taken seriously by authorities (Bobo, 2011). Do the cameras and sensors in restaurants focus on preventing employee theft of food, stopping food poisoning, and/or catching safety violations? Does "traffic control" include efforts to stop honking of horns and loud motorcycles late at night in urban neighborhoods, or is that health-damaging noise deemed just as unworthy of computational scrutiny as it is casually excused by millions of small acts of policing discretion each year — as opposed to the charge of "blocking pedestrian traffic" that is commonly used by police as an excuse to harass African-Americans standing on empty sidewalks (Taibbi, 2014)? Would autonomous car control systems prioritize preventing pedestrian deaths, or merely aspire to smooth flows of cars into and out of the city?

The ideology of neoliberalism all too often provides rapid, "obvious," and unchallenged answers, based on dubious cost-benefit analyses. Its *summum bonum* is to improve the business environment and spread market logics to all dimensions of human life. Yet problems multiply even within the neoliberal framework, particularly as it expects state actors to realize business goals (and vice versa). The state itself must capitulate to (and coordinate) its subjects' purported emancipation from it. So, as Philip Mirowski argues, there is a neoliberal pattern of "hav[ing] it both ways: to stridently warn of the perils of expanding purview of state activity *while simultaneously* imagining the strong state of their liking rendered harmless" [15]. These tensions are a formal feature of ideological thought: it is a way of containing and coordinating commitments that are contradictory either in theory or practice (Geertz, 1973).

Although these ideological beliefs are most often pegged to Wall Street and Silicon Valley, they can be found, without much difficulty, in even our highest legislative bodies. In February 2015, the United States Senate held a hearing called "The Connected World: Examining the Internet of Things" [16]. The hearing featured statements from senators and testimony from a panel of five witnesses. The attitudes throughout were overwhelmingly excited for the smarter lives we will all be leading thanks to the IoT. While there were occasional mentions of basic issues related to security and privacy, most of the concern stemmed from worries about "over regulation," which meant anything more than a “light touch” approach. In his statement, U.S. Senator Cory Booker (D–NJ) neatly encapsulated the political economic ideology on display in the hearing — and while he was more enthusiastic and explicit in tone than others, his remarks are representative and worth quoting at length:

> “This is a phenomenal opportunity for a bipartisan, profoundly patriotic approach to an issue that can explode our economy. I think that there are trillions of dollars, creating countless jobs, improving quality of life, [and] democratizing our society in ways that gives advantages to people who are being marginalized on the edges, breaking down barriers of race and class. We can’t even imagine the future that this portends of, and we should be embracing that ... And so a lot of my concerns are really what my Republican colleagues also echoed — which is, we should be doing everything possible to encourage this, and nothing to restrict it ... But for us to do anything to inhibit that leap in humanity to me seems unfortunate ... And I also believe that this should be a public-private partnership. We all have a role.”

Booker’s statements are not radical. He is in fact channeling the mainstream views about innovation in society. The least we can do is get out of the way. At best, our duty is to provide all the legal, material, and ideological support we can for innovations — and their innovators — like the IoT. Anybody who wishes to ask critical questions about the future, let alone actually constrain and slow down technological development, is *de facto* extinguishing an exploding economy and standing in the way of a democratizing force for justice.

Booker’s language recalls the puffery of finance capital — the same group he vigorously defended in 2012 after the leader of his political party (Barack Obama) gently suggested the possibility of ending private equity tax loopholes. Overclaiming the value of the smart city is vital to contemporary capital markets, since extreme inequality in wealth allows rentiers to live well even on the very low interest rates offered by nearly risk-free sovereign debt. The “smart money” probably will understand the “smart city” as an even more speculative bet if it peruses security experts’ warnings about the security problems now endemic in the Internet of Things. (As Bruce Schneier (2014) has observed, when computing is embedded into hardware (as is the case in most of the IoT), sensors and routers are “riddled with vulnerabilities, and there’s no good way to patch them”). The riskier the investment, the more spectacular the potential gains must be: thus the proliferation of characterizations of smart city technology as epochal, groundbreaking, world-making.

Of course, the rhetoric is not always so grandiose — there are cross-cutting, technocratic pressures to sound cool, analytical, and mechanically objective when describing new technology. Bland bipartisanship is also a favored rhetorical mood. Boosters lard manifestos, manuals, and exhortatory books with simple, straightforward examples of problems all can agree need fixing (Newsom, 2013; Townsend, 2014), in order to obscure the stakes of automated surveillance and regimentation of every moment and place. A pothole-spotting app, for instance, is a step toward at least informing (if not guaranteeing the filling of) an unmitigated, car-harming bad. But not everyone agrees with, say, Goldsmith and Crawford when they argue for “postprogressive” city management that focuses on “results not compliance” [17], once the “results” desired move far beyond fast trash pickup or smooth roads. Indeed, the very choice to deploy resources for road smoothing (rather than, say, train or bus air conditioning, or green spaces) is an inherently political one. Goldsmith and Crawford celebrate a new, “smart” fingerprinting initiative aimed at criminals [18], with nary a reflection on the ways in which these records databases create underclasses of effectively unemployable individuals.

Smart city advocates may counter that such conflicts over resource allocation are inevitable in any political order, and stress that their own deployment of sensors, apps, open data, and progress reporting cannot be expected to unravel them. But realities of scarcity apply to political attention, problematization, and action as well. Time spent organizing to deploy a “platform for citizens to engage city hall, and each other, through text, voice, social media, and other apps” [19], is time not spent on highlighting the role of tax resistance by the wealthy in *creating* the very shortage of personnel that smart cities are supposed to help cure by “force multiplication” of the cities’ remaining workers (Winters, 2011; Bady, 2013). Would Newark, New Jersey, need Mark Zuckerberg’s donation of US$100 million to its school system, if so many others in the billionaire class had not fought so hard to reduce their own (and corporate) taxes, shelter wealth abroad, and defang regulation? Each time a “quantrepreneur” proposes ingenious new ways of measuring and maximizing the “output” of government workers, a critical citizenry should ask: how did we come to this pass? Where has the constant pressure to “do more with less” come from? Focusing on the tech of “doing more” displaces critical debate on the why of “less” governmental resources and employees.

The corporate and governmental actors behind the smart city ideal have distorted debate in two ways. First, focusing on the narrow goals of promoting transparency and efficiency, they have obscured the revolutionary changes in law enforcement's intensity, scope, and punitive impact portended by pervasive surveillance systems that are easily embedded into a regime of ambient law. Second, they offer a doubly crabbed view of the politics and ethics of digitizing space via the IoT: as a *post hoc constraint* imposed on technical systems, primarily to encourage "privacy," in the individualistic sense of the right to control the collection of information about oneself.

By applying a hermeneutics of suspicion, a more complete — and troubling — social theory of the smart city emerges. Even at the least intrusive end of the spectrum of control enabled by the IoT, there is far more at stake than the nebulous set of concerns about perception and reputation traditionally encapsulated in the umbrella term "privacy." And at the far end of control, the stakes are very high. The IoT is not simply a chance to *watch* people, but to produce and reproduce certain patterns of interaction (Bogard, 1996), and to *replace* people with robotic agents once data about them has been so pervasively recorded that it can be downloaded into an automaton to simulate their actions.

IV. Smart cities in societies of control

What will a social theory of the smart city demand? As opposed to the ideology of advocates, social theory is a "systematic, historically informed and empirically oriented theory seeking to explain the nature of 'the social,'" where the social "can be taken to mean the general range of recurring forms, or patterned features, of interactions and relationships between people" [20]. To take on ideal-types of interactions in urban environments, critical patterns include relationships of allocation/extraction, oppression/emancipation, and recognition/misrecognition (Fraser, 1995). Close examination of the phenomenology of being a surveilled subject, a data subject, reveals the vulnerability of each resident of the smart city to extraction, oppression, and misrecognition.

In many ways, Foucault's concept of biopower has explanatory fit. One form of biopower is, he writes, "centered on the body as a machine: its disciplining, the optimization of its capabilities, the extortion of its forces, the parallel increase of its usefulness and its docility, its integration into systems of efficient and economic controls, all this was ensured by the procedures of power that characterized the *disciplines*: an *anatomo-politics of the human body*" [21]. In contrast to the modes of sovereign power that exercised the right "to *take* life or *let* live" [22], the modes of disciplinary biopower exercise the ability to administer and manage bodies and populations. The smart city not only operates on people in this way — for instance, viewing citizens as analog-*cum*-digital information nodes, or "citizen sensors" [23] — but it also reimagines and reconstructs the city, in itself, as a machine, which can and must be administered and managed. One theorist, inspired by Foucault's concept of "governmentality," has deemed this type of disciplining "smartmentality" (Vanolo, 2014).

While the concept of biopower is certainly illuminating, it doesn't give us the full picture. We can reveal more about the smart city by applying a different social theory — one that explicitly sought to succeed Foucault's disciplinary societies, just as Foucault's model succeeded the "societies of sovereignty" — namely, Gilles Deleuze's (1995) notion of "societies of control." If the sovereign power was, as Foucault points out, symbolized by the sword, and disciplinary biopower was represented by industrial machines, then control corresponds to computer networks (Deleuze, 1995). Now, of course, the existence of one mode of power does not abolish the others. Rather, it is a question of which one is the dominant operational logic. And, when applied to ICT, especially the networked technologies of smart cities, Deleuze's framework makes clear the common logics underlying these practices and ideologies. We will provide a preliminary application of this framework to demonstrate its merit as a social theory of the smart city.

A Deleuzian "society of control" has at least three crucial components — dividuals, rhizomes, and passwords — which come together to form a continuously acting logic.

When one person observes another, a basic perceptual apparatus of sight and vision demands at least some minimally holistic assessment. It is hard to register what a walking person is wearing, for example, without also noticing gender, if the person limps or strides, is tall or short, among the hundreds of other bits of tacit knowledge that may be conveyed by an appearance. Monitored by sensors, by contrast, city dwellers are becoming less individuals than "dividuals": entities ready to be divided into any number of pieces, with specific factors separated, scrutinized, and surveilled. What the *person* does becomes less important than the consequences calculated in response to emanated data streams. For example: the metadata from a phone call may be far more fateful than the talking which we usually take to be its purpose.

With digital technologies, the individual is atomized, blown apart into streams of data fed into processors. And as these sensors gain immediate influence over physical objects like doors, fences, and automobiles, there is little to no chance of the communicative dialogue that is a hallmark of human interaction. Instead, these relations are at their core *strategic*, in the Habermasian sense, rather than communicative (Habermas, 1984). Consequences will result not from the "unforced force of the better argument," or even coaxing and cajoling, but rather, by force alone, as programmed by a set of managers and software developers far removed in time and space from particular implementations of programmed rules [24].

For example, facial recognition software enrolls a person's face, and by extension the person it is associated with, into a network, whether the person wants to be enrolled or not. Hackers now claim they can even use photographs to identify fingerprints as well (Santus, 2014), a potentially massive boon for law enforcement. The health wristband paints a picture of a self by collecting and analyzing somatic data. The location-tracking sensor registers geospatial coordinates. The Department of Homeland Security's Cell-All initiative senses "deadly" chemicals. The RFID reader only cares about the chip in your wallet. The biometric lock is only concerned with your fingerprint or irises. The list of ways that people are dividualized goes on. It is identity via synecdoche, where a factor — which factor depends on the system — becomes representative of the whole and becomes all that matters.

The array of underlying technical systems, which are often hidden from sight and mind, can be conceptualized as what Deleuze calls a "rhizome" — like the roots and shoots of a persistent, massive set of plants, it seems to pop up everywhere. Rhizomes are assemblages of concepts, relationships, materials, and actions. They have no distinct boundaries; rather, they are fluid fields, always acting, pulsating power, emanating from multiple directions with varying intensities. The city's networked, 'smart' technological apparatus can simultaneously be: sensing chemicals in the atmosphere; tracking bodies as they move through space; surveilling the types of faces on the street; sending police to remove unwanted people; moving traffic along the roads; and more.

Even as a swarm of disconnected, "dumb" machines, this emerging rhizomatic apparatus of monitoring and control can be intimidating. No one wants to be on the wrong side of its algorithms. As urban technological networks grow vaster and more interconnected, secondary uses of data barely imaginable at the time "users" begin participating in the IoT may well become commonplace (Hoofnagle, 2003). Data gathers and brokers — from corporations to governments — will find a plethora of uses for the information. Consider the biometric lock: Surely the times, places, and identities of who is granted access will be categorized and logged, but what might be even more interesting to authorities is the data for who is denied access.

And people-*qua*-dividuals have freedom only insofar as all their "passwords" — the products of dividualization that mark access or restriction, allowing one to move freely through or be stymied by the rhizomatic system — are in working order. (Do you wish to enter through a keypad lock? Your PIN is the password. Do you wish to purchase something? Your credit card is the password.) Life is filled with these passwords. Yet, at any moment a password could be rejected — rightly or wrongly, with or without your knowledge — and the amount of control the array of underlying mechanisms have over you become bluntly apparent. Deleuze asked us to imagine "a city where one would be able to leave one's apartment, one's street, one's neighborhood, thanks to one's (dividual) electronic card that raises a given barrier; but the card could just as easily be rejected on a given day or between certain hours" [25]. As infrastructure decays and the rhizomatic tendrils extend further, city dwellers increasingly feel the Kafkaesque frustration such a scenario entails.

Technology critics often portray these unexpected developments in technological control as a kind of Frankenstein's monster or sorcerer's apprentice, one that "we" have unleashed via thoughtless adoption of technology [26]. Social theorists must push the question of causation and agency further, identifying the powerful *actors* who remain above the fray of dividualization, weaving a web of forces that increasingly constrain the time and space of city dwellers (Krieger, 1994). Masses may be consenting to be dividualized, but only a few wrote those terms and enforce them (Rothkopf, 2009).

Through Mirowski's detailed analysis of the cause and context of the financial crisis, we can see how these 'smart' initiatives plug into the ideologies and tactics of neoliberal political economy: "Technocratic elites could intently maintain the fiction that 'the people' had their say, while reconfiguring government functions in a neoliberal direction. These elite saboteurs would bring about the neoliberal market society far more completely and efficaciously than waiting for the fickle public to come around to their beliefs" [27]. The distinction between control and consent is important to several recent initiatives toward the creation of smart cities. Pervasive interlinking of surveillance/sensor arrays, computational processing, and virtual databases into the physical structure of cities is only legitimate if citizens can, both politically and in individual encounters, can be said to have "consented" to it. But when that consent is remote or indirect, its force, validity, and scope should be vitiated. Internet "terms of service" are the ideal-type of desiccated, hollow, *pro forma* "consent" that is better termed obeisance, acquiescence, or learned helplessness. Thus the overall pattern of relationships in the smart city results in a seamless "spectrum of control," with meritorious or merely creepy technologies directly imbricated with deeply disturbing ones.

The idea of a "spectrum of control" is more than a turn of phrase [28]. It serves as a symbolic visualization of an interpretation of a text — here, the text is the city, considered simultaneously as a kind of aesthetic object and software program. As Charles Taylor has stated, in canonical work on interpretive social science, interpretation “is an attempt to make clear, to make sense of an object of study” that is in “some way confused, incomplete, cloudy, seeming contradictory — in one way or another, unclear” [29]. Just as skilled commentators can interpret literature, judicial opinions, and works of art, we should take the city’s increasingly technologized systems of governance as expressive texts in need of interpretation.

Both the rhetoric of the “smart city,” and the actual city itself, are texts and text-analogues. They are cloudy and confused now because so much theoretical effort has gone into separating out wheat and chaff, to minimize “coercion” and maximize opportunities for “consent.” This well-meaning, but ultimately futile, normative agenda contributes to confusion and contradiction because the IoT and all-pervasive surveillance are building less a *smart city* than a *cyborg city* (Gandy, 2005) — urban places where the stakes of access to certain prosthetic extensions of the self are ever rising. In such cyborg cities concepts like consent vs. coercion, control vs. autonomy do not exist as binaries — but rather they exist on a continuum. Shoehorning the daily experience of the smart city dweller into such binary choices will only further falsify the lived experience of urbanites. Economic pressure toward a “full disclosure future” [30] makes opting out a luxury good (Angwin, 2014).

By theorizing in terms of a spectrum of control we can draw connections between technologies that were before thought of as discrete and independent. The innocuous is enfolded with the menacing. Any significant technology of the smart city becomes a tool to be repurposed for later, often-unforeseeable goals. Claude Lévi-Strauss has compared human thought processes to the work of the handyman, or bricoleur, who fixes problems as best he can with whatever tools or materials are lying at hand (Lévi-Strauss, 1966). A similar process of bricolage will embed technologies of the smart city into solutions proposed for problems large and small — and will, in turn, help define what is viewed as a problem properly solved by the polity.

V. The soft power of biometric surveillance

At one end of the spectrum of control are the technologies that enact their power in subtle ways. They are increasingly ubiquitous and become subsumed into the background of everyday life due to their ‘invisibility’ (Star, 1999). That is, they can be functionally invisible because people no longer notice their relationships and interactions with the technologies and/or physically invisible because they are intangible or hidden.

Political philosopher Giorgio Agamben [31] explains this particularly curious mode as an “operation of power that does not immediately affect what humans can do — their potentiality — but rather their ‘impotentiality,’ that is, what they cannot do, or better, can not do.” Through this way of operating, power is not limiting my capacity to do an action — in the conventional way of constraining subjects — but instead is making it very difficult for me to *not* do an action. For example, when few people had cellphones it was easy to not own or use one, but now that almost everybody does — and increasingly more parts of our life our tied to the constant communication and platform capabilities afforded by the device — it’s nearly impossible not to also conduct your life via a cell/smartphone (Peppet, 2011; Morozov, 2014). The same can be said of automobiles: nothing forces any given person to buy an automobile, but when infrastructure is constructed with private vehicles assumed, and when there are scant other alternatives, it becomes difficult to *not* make the choice.

Urban surveillance technologies — especially as they are implemented as part of massive, networked systems — anchor the subtle end of the spectrum of control. Consider the closed-circuit television (CCTV) arrays that already blanket the streets and buildings of major cities around the world. CCTV is now emerging as a kind of “fifth utility” within cities (alongside gas, electricity, water, and telecommunications). “Once CCTV systems are installed, their logic is inevitably expansionary. Economies of scale are very marked — once a system is built and monitoring personnel are employed, it makes sense to cover larger and larger areas” [32]. In the ‘smart city,’ such surveillance systems rush down the path towards ubiquity; they become subsumed into the background of everyday life: always present, tirelessly watching, but rarely noticed.

CCTV is a flexible technology, with the potential for added layers of sophisticated software incorporated into the hardware — such as biometrics that are linked to the in-depth, personal information held and managed by data brokers. The proliferation of surveillance systems as part of ‘smart’ initiatives, which are then enhanced by advanced analytics, changes the very political economy of what it means to be a city dweller.

Let’s consider further the example of biometrics, which identify, measure, and collect a biological trait or group of traits [33]. There are a wide variety of types of existing biometrics, with more in development. Some of the most common focus on physical traits: faces, fingerprints, irises, retinas and DNA. Others focus on behavioral traits: voice, signature, gait (how a person walks) and keystrokes (speed and timing between key presses). In practice, biometric technologies employ a standard process across different types. A sample of the biological trait is collected using a sensor of some kind, such as a camera for faces or a telephone for voices. Through the use of an algorithm that extracts information from the biometric sample, the trait is then converted into a digital representation called a "template," which can be stored in a database. The larger the database, the more templates there are to verify or identify subjects. The key component, though, is the algorithm used to construct the template. This is the feature that distinguishes one biometric recognition system as 'better' than others on markers like: can the algorithm quickly extract biometric information? Can it do so in a variety of environmental circumstances? Can it create a template that is accurate?

The potential role of biometrics in the information economy is huge — especially for the massive data-brokerage industry. During a 2013 U.S. Senate hearing, Senator John D. Rockefeller IV, then Chairman of the U.S. Senate Committee on Commerce, Science and Transportation, said: "In 2012, the data broker industry generated $156 billion in revenues. That's more than twice the size of the entire intelligence budget of the United States Government — all generated by the effort to learn about, and sell, the details about our private lives." [34] Biometrics present new ways to convert data into profit, a figurative strip-mining bodies (and their actions) so that ever more actionable information can be extracted from them. This analogy captures the degree of intrusiveness that biometrics have when they hone in on particular biological traits and pull them out of the context of the rest of the body, person, and environment.

The finer grain, personalized data provided through biometrics would be like gold in the data brokers' servers, enabling companies to significantly fine-tune the way they target potential customers and providing government agencies with additional ways to oversee populations. "Despite consumer data broker companies' clear links with credit rating agencies, revenues numbering in the billions, exemption from state regulations to protect consumers from identity theft, and documented data breaches, the average citizen has likely never heard of these powerful corporations" [35]. Since these brokers collate data and construct profiles through whatever means available, by adding biometric algorithms and databases to the mix, these brokers, and crucially their clients, accumulate troves of data to the point that they may know more intimate details about persons (including income, debt, illness, criminal records, and drugs taken) than their families do. Some high-end stores already use facial recognition software to alert clerks and salespeople that a VIP or a celebrity is in the store (Salinas, 2013). With large enough databases, what's to prevent stores from identifying even non-VIP customers who walk in the door?

The acceleration of profiling and personalization is a natural consequence of big data business strategies. Firms at the center of the big data economy claim that their data troves reverse the common economic law of diminishing marginal returns. The more data a firm has, the more its existing store is worth, since contextualization of profiles enables ever greater power of sorting, control, price discrimination — and even blackmail.

These implications, among others, are consequences of the ways biometrics allow — and encourage — more intensive commodification of physical bodies. "Biometrics break bodies down into their component parts in ways that allow them to be marketed more easily in the transnational marketplace ... The flimsy material body is rendered rugged as biometric technologies make the body replicable, transmittable, and segmentable" [36]. We've heard of the data economy, but how about the face economy, or iris economy or gait economy? There are entire corporate sectors eager to mine that data and put it to use in any number of ways: data brokers construct in-depth consumer profiles replete with biometric templates; salespeople and store security use biometric emanations to pull up your reputation from the database; and your identity is pinned to your location, which is better tracked as you move through the streets, public squares and shops. Insurance companies, for instance, are hungry for the somatic data provided by personal health and fitness monitoring devices (Sadowski, 2014a). Imagine what they, and others, could do with the knowledge and power provided by diverse types of biometrics.

Thus, biometrics present a way to not only dividualize people at minute scales, but also provide the means to intensify commodification — via strip-mining the newly available sources of data — and control — via biopolitical management — of people, all while the 'smart city' constructs a conducive platform for these activities.

The technological systems installed within cities to make them more connected, efficient, secure, and smart don't exist in a vacuum. They "absorb and reproduce the dominant cultural values of the contemporary political economy" [37]. At the subtle end of the spectrum of control, the systems act on us in ways that are functionally and/or physically invisible; few even know about data brokers, intrusive surveillance, and the ways we become incorporated into the data flows of capital. And even then, we "consent" by default because the options to *not* do things that pull us into the logics of these systems — such as not using digital platforms, not using smartphones, not going to stores and streets without a mask, not living in a populated area — can hardly be considered real choices for the vast majority of citizens.

VI. The hard power of policing technologies

On the other end of the spectrum are technologies of control that enact their power in aggressive, violent ways. Consider how the current tactical and technological trends of urban policing are consolidating power in security and enforcement agencies. An increasing number of highly publicized protests from around the world have had the side effect of revealing — and ramping up — some of the suppression methods state forces are employing when confronted with an organized public. The police responses to protests — large and small, peaceful and riotous — are often severe and militarized (Balko, 2013).

Clashes between protesters and police at Occupy (in hundreds of sites in the U.S. in 2011, and in Hong Kong in 2014) and #BlackLivesMatter (in the wake of the Darren Wilson and Daniel Pantaleo grand jury decisions) escalated from ordinary policing to paramilitary pacification, sometimes in a matter of minutes. Such footage could easily be confused with a battalion of troops holding the line against insurgents in the urban battlespace [38]. The science of protest management — replete with "sublethal weapons" like ear-paining long-range acoustic devices (LRADs) and nerve-damaging, plastic handcuffs — typically manages to disperse the crowd in short order. Violent and even sexualized harassment is also distressingly common. When challenged verbally, authorities all too often double-down and wield physical force to impose order. Riot gear, rifles, tasers, pepper spray, dogs, water cannons, tear gas, monitoring, tracking, and arrests have all become normalized for authorities.

Smart city technology could make the control of protests less physically violent, but ever more precise and effective as a deterrent against collective action. In January 2014, protesters in Kiev, Ukraine received an ominous mobile phone message from state authorities: "Dear subscriber, you are registered as a participant in a mass riot." That charge — thanks to tough new Ukrainian laws against public gatherings — can come with a sentence of 15 years in prison (Walker and Grytsenko, 2014). These tactics are indicative of a move towards using technologies that break-up protests — or even prevent them from happening in the first place — using a purely technological intervention. The psychological effects go well beyond immediate confrontations. Just knowing it's possible to be arrested, at home or work, days after attending a protest — all thanks to remote registration in police and homeland security dossiers — is enough to thin out the activist ranks. Or they may (as in the case of Ukraine itself) raise the stakes to the point that protesters feel compelled to revolt, given dark possibilities of collective punishment if the regime entrenches itself. Once again, the stakes rise very quickly.

As Paul Virilio warned in "The state of emergency," rapid pacification of threats can, in turn, lead to an arms race in the intensity of threats. He has observed that "the reduction of warning time that results from the supersonic speeds of assault leaves so little time for detection, identification and response that in the case of a surprise attack the supreme authority would have to risk abandoning his supremacy of decision by authorizing the lowest echelon of the defense system to immediately launch anti-missile missiles" [39]. Similarly, as protesters began to anticipate and evade blunt crowd dispersal tactics, the leaders of a pervasively "smart city" would be tempted to embed algorithmic deterrence into transport and policing systems. That creates a dangerous dynamic among protesters: for while some may simply give up, others may, along the lines of the Ukrainian model, decide that one should only strike the king with a killing blow — that is, the only politics worth engaging is the complete overthrow of regimes determined to disadvantage peaceful dissenters. The reformist space of democratic politics and collective action evaporates between the poles of quiescence and revolution.

At present, "smart" crowd control technologies buttress acquiescence. Consider the work of the firm Persistent Surveillance Systems. Police in the United States have begun to test the company's services, which use a civilian aircraft that allows authorities to cast a wide surveillance net across the city (Friedersdorf, 2014). The company's owner likens it to "a live version of Google Earth, only with TiVo capabilities" (Campbell-Dollaghan, 2014). The technology lets police record, rewind, and zoom aerial video so they can track the movements of specific vehicles and people within the city. The crowd control potential of having a real-time and recorded eye-in-the-sky is vast. The escalation of tracking capabilities isn't surprising or new. It's another layer on top of the extensive technologies already deployed.

The spread of wide-area, networked surveillance systems are a solid foundation and complement for the next phase in automated law enforcement. As a group of academics — many of them from the U.S. Military Academy at West Point — warn in a recent article, the typically manpower-intensive methods of policing are undergoing technological changes. By delegating police activities to technological systems — like algorithmic analyses, robotics, and broad-spectrum sensors — opportunities for dissent and protest are minimized. Any response by citizens becomes defanged. These "automated systems scale efficiently, allow meticulous and tireless enforcement of many laws, promise rapid dispatch of punishment, and offer financial incentives to law enforcement agencies, governments, and purveyors of these systems" [40].

Now consider the likely, near-term possibility that authorities will aggressively deploy drones and robots to "deal with" protesters. For instance, the South African company Desert Wolf has developed a riot-control drone they call the Skunk, which is armed with a veritable arsenal of "sublethal" capabilities. Along with strobe lights, cameras, and speakers, the Skunk comes equipped with four paintball guns that can be loaded with "dye marker balls, pepper spray balls or solid plastic balls" in order to "disperse or mark people in the crowd" (Doctorow, 2014). The Skunk is first being delivered to mining industries to deal with employee strikes. Extending that logic to urban protests is not difficult, since the logic is ultimately the same in both cases: subduing those who seek to interrupt and change the current structures of power and capital. After all, by using some version of the Skunk police forces can deal with dissent in ways even more effective, flexible, dehumanized, and safe (for them). Calibrated robotic and drone interventions may eventually become part of the furniture of 'smart' urban existence where all glitches in the city system are problems in need of techno-fix responses — assumed as legitimate when used against protesters and drug dealers alike.

And the power of "non-violent" police tactics is growing. Technological means threaten to even prevent crowds from forming in the first place, thus moving from reactionary to prophylactic strategies. San Francisco authorities manipulated both train schedules and wireless access to disrupt protests. New York's MTA has simply forced trains to bypass stations where protests are occurring, to keep people from assembling. Police power to surveil large areas, use remote scare tactics, automate escalation of enforcement, and even practice what's being called "predictive policing" is supposed to lead to a more orderly society [41]. To the extent such measures deter legitimate protest, they entrench a more mechanized, inorganic society — one where surveillance is used to capture, and replay, one set of power relations, over and over again. The *body* politic mummifies into a very different type of social organization: a leviathan *machine*.

The result is a self-reinforcing sense of alienation and passivity. An underclass is created, whether materially, politically, or (most likely) both. The subjects of the smart city are simply herded along toward maximally productive activity (via nudges or shoves), rarely if ever given the time to questioning the how or why of their own opportunities or aspirations. When big data is touted as a way to understand and control society without sufficient attention to the history (or patterns of thought) that gave rise to the data analyzed, it is set to rationalize unjust patterns of extraction and discipline. A finance firm may say, for example, "we charge 15 percent interest to someone who had a past default, just because past patterns of data show that such people often default again," in a process agnostic as to whether a defiant refusal to repay, or a family medical emergency, caused the prior default. Similarly, the police may say, "we're intensively policing this neighborhood because it had 10 percent more crime in the past." But what if defaults resulted from excessive interest rates in the past, caused by discriminatory lending practices? And what if the above-normal crime rate in the neighborhood simply reflected past patterns of intense policing that reflected racism? What if each decision makes future defaults, or excess crime rates, more likely? Then the "science of society" promised by big data morphs into a subjugation of certain parts of society. The algorithms behind such judgments become less "objective arbiters" of opportunity and punishment, than ways of laundering subjective, biased decisions into ostensibly objective, fair scores. Those affected lose a chance at individualized treatment and understanding, as technical systems treat people as a mere collection of data points.

Stephen Graham argues, in a 2011 interview with *Democracy now!*, that cities are the "foundation space for democracy." They can be thought of as a staging ground for public reactions and protests — a spotlight on larger social issues. Yet, transforming urban space into a highly technologized, secured environment reinforces and normalizes the view that anything but subdued acceptance of the status quo is unwelcomed, and thus must be contained and stopped. In his book *Cities under siege*, Graham (2011) argues that the capacity for democratic action is under attack. He writes, "Militarized police cordons, often supplemented with pre-emptive detentions and bans on the right to protest, try — often violently — to confine protestors for long periods in space where they have little exposure to the media and few opportunities to communicate their political message" [42]. In short, the actions of protestors and whistleblowers, activists and advocates, are not always valued as integral parts of a flourishing society. That can be just as dangerous as the activities protesters, properly, try to expose, call attention to, and deter.

Such trends in policing tactics and technologies are not necessarily caused by smart cities — they are certainly occurring in places not touched by 'smart' initiatives — rather, the smart city opens the door for new ways to intensify and entrench them. When urban infrastructures are rigged with networks of surveillance, sensors, and algorithms, the ability for police forces to monitor city spaces and mobilize action is enhanced. Such secondary uses of data render nugatory whatever initial "consent" was given to the data collection that enabled them. Even more importantly, they threaten to expand the boundaries of what counts as disorder and amplify the reaction to any efforts to object to further militarization.

VII. Cyborg urbanization, blurred boundaries

These technologies of control, on both sides and the spectrum, gain efficacy because — perhaps now more than ever before — the boundaries between body–city–technology are blurred. There are not so much discrete entities — the person, the building, the device — as there are entangled assemblages of flesh, concrete, and information. And these connections amplify the ability of those in power to coordinate and channel apparatuses of control throughout the rhizomatic assemblages. The modern city, then, has to be theorized in terms of "cyborg urbanization." The city dweller is better understood as an urban cyborg: one who doesn't live *in* the city, but who lives as *part* of the city. As geographer Matthew Gandy puts it,

> The emphasis of the cyborg on the material interface between the body and the city is perhaps most strikingly manifested in the physical infrastructure that links the human body to vast technological networks. If we understand the cyborg to be a cybernetic creation, a hybrid of machine and organism, then urban infrastructures can be conceptualized as a series of interconnecting life-support systems. [43]

The infrastructure provides for human needs: running water; climate controlled environments; food preparation and delivery; routes for mobility and transportation; places for social gathering. Disruptions after disasters like Hurricane Sandy remind us of just how fragile these systems can be and how deeply we are wrapped up in them. But just as we think of the role physical architecture plays in guiding and sustaining city dwellers, we must now also think of the role software architecture has in city governance.

As people become urban cyborgs, bodies merged with cities, our interfaces with the system grow more entangled. The libertarian fantasy of the cyborg envisions the human as an island: armored with an exoskeleton, temperature and blood sugar levels automatically maintained, the *über*-robot wants for nothing, fears nothing. However, the health of the individual depends on the health of the sociotechnical collective. And the move from analog to digital infrastructures has only deepened this integration. Such technologies exist ubiquitously and invincibly. The watchword here is "natural user interface," which aims for frictionless interaction. It portends cybernetic existence without kinetic interference. The urban cyborg's life is mediated and structured by technologies in ways large and small, obvious and unnoticed.

In the "Cyborg manifesto," Donna Haraway [44] wrote, "No objects, spaces, or bodies are sacred in themselves; any component can be interfaced with any other if the proper standard, the proper code, can be constructed for processing signals in a common language." Part of her project here was to map the large-scale "transitions from the comfortable old hierarchical dominations to the scary new networks" she calls "informatics of domination." Similarly, Deleuze [45] said, "We're moving toward control societies that no longer operate by confining people but through continuous control and instant communication." For him, this transition corresponds with "cybernetic machines and computers," yet we must also realize "the machines don't explain anything, you have to analyze the collective arrangements of which the machines are just one component." These interventions from Deleuze and Haraway suggest a techno-political logic of cyborg cities more menacing — but potentially more emancipatory — than the bland technocratic meliorism of "smart cities." If we can see ourselves as part of a cyborg city, simultaneously wholes and parts of a whole — not only interacting with the rhizomatic urban assemblages, but as part of them — the valence of the cyborg metaphor shifts. The "body politic" takes on new meaning.

The cyborgification of city life raises critical questions about an interlocking series of existential and social questions. Computerized implementation of rewards and penalties, welfare and policing, are premised on a series of decisions as to whether any given (in)dividual should be controlled, or granted opportunity; should be invested in, or treated as a site of extraction. Existentially, the city dweller must decide whether to compete for investment, or to challenge existing power structures, or simply to drift, swept along by the decisions of those who create the circumstances that others merely endure.

And as our lives increasingly take place within "coded space" — spaces that are augmented by digitally inscribed information — and "code/space" — spaces that are so infused with information that it is a necessary component of their functioning — the power of computerized processes becomes even more pervasive and inescapable (Kitchin and Dodge, 2011). While the term *code* can connote law (as in the Internal Revenue Code) or software (which involves the "coding" of instructions into machine-readable formats) (Lessig, 1999), it can also suggest a deliberately hidden meaning. Someone sends a "coded message" in order to avoid detection, to keep third parties from understanding exactly what is going on. In algorithmic decision-making, this third, mysterious aspect of code too often predominates. For example, with credit decisions, there are so many vague or conflicting codes that it is possible to rationalize virtually any move of a credit score after many credit events. Maybe you have too many accounts open, maybe you have too few — either could contribute, at any given time, to a decision to reduce a credit score or reject an application. The answer to *who* is making decisions that dictate access, resource distribution, mobility, and more, is opaque — because the correct question might be *what* is making those decisions.

With all the optimistic promises and hopeful visions surrounding 'smart cities' it can be easy to lose track of the politics that are coded into these interconnected technologies and initiatives. If we conceptualize these urban transformations as merely neutral enhancements that bring unalloyed goods of efficiency and security, then we miss out on the socio-political, even ontological, aspects of what it means to be entangled in these rhizomatic mechanisms, assimilated deeper into the functioning of the cyborg city, and controlled by algorithmic decisions and technologically extended force.

VIII. Taking back control

We expect that our analyses of politics in the smart city and our re-interpretation of its sociotechnical assemblages as a cyborg city should have normative import. Within the context of the "spectrum of control" we can derive support for the principle of "the right to the city." This right originated from Henri Lefebvre as a means for people to take back the urban social space by challenging the abuses of capital through a re-imagination of the duties and prerogatives of citizenship (Purcell, 2002). In the context of globalized neoliberal and technocratic ideologies, such a right then takes on new importance — and serves as a rallying call for challenging the technologies of control that proliferate and engulf us.

David Harvey, in his landmark paper on the subject, forcefully explains what the right to the city entails:

> The question of what kind of city we want cannot be divorced from that of what kind of social ties, relationship to nature, lifestyles, technologies and aesthetic values we desire. The right to the city is far more than the individual liberty to access urban resources: it is a right to change ourselves by changing the city. It is, moreover, a common rather than an individual right since this transformation inevitably depends upon the exercise of a collective power to reshape the processes of urbanization. The freedom to make and remake our cities and ourselves is ... one of the most precious yet most neglected of our human rights. [46]

This type of plasticity is not simply a matter of ensuring a living wage, or some bare subsistence standard of living, for all in the "smart city" — however crucial such measures are. Rather, it is a critical aspect of human freedom, if the term is to have enduring meaning in an environment where corporate and government actors are honing ever more sophisticated means of monitoring, control, and manipulation (Unger, 2004).

Julie Cohen has sketched a broad outline of further normative responses to the rise of smart technologies and networked intelligences. Resisting the big data logic, that more data is always better, she pursues "semantic discontinuity" between different knowledge gathering and parsing systems (Cohen, 2012). The pursuit of complete interoperability, legibility, and access between data systems must be closely interrogated, and often blocked.

The grim results of overreach are already clear. For example, vertical integration of municipal, state, and federal law enforcement data, plus horizontal joinder of intelligence and investigative systems of military and police forces, in the United States (via the fusion center apparatus), resulted in a series of snafus and civil liberties violations with little if any discernable impact on public safety (Citron and Pasquale, 2011). Early, clumsy efforts at health data integration in the U.K. outraged patients when authorities decided to sell the data to insurers. Each of these episodes should serve as a cautionary tale for the would-be architects of smart cities: without consistent citizen consultation and serious penalties for misuse of data, their apparatus of omniveillance could easily do more harm than good.

The smart city's legitimacy also depends on its even-handedness. There are curious gaps in this apparatus of control. Somehow, certain corporate lawbreakers are rarely, if ever, monitored, let alone punished. By contrast, the average person is dividualized by the rhizomatic apparatus because the dividual can be better analyzed, penetrated, and controlled. As Jonathan Crary's (2013) *24/7: Late capitalism and the ends of sleep* shows, the military logic of eternal vigilance is gradually filtering into capitalist assumptions about work and subsistence wages. If the shift towards smart cities provides a technocratic rational for governments to dutifully double down on entrepreneurial forms of governance (Harvey, 1989), they will deserve resistance. Merely serving as "political-technological assemblages designed to naturalize and justify new assets for the circulation of capital and its rationalities within cities" [47], the sensors of the smart city will amount to little more than a technologized re-imposition of old chains.

Commentators have already observed the resurrection of early capitalist piecework in the guise of a "gig economy." Planners should acknowledge that slavery was not a deviation from capitalist imperatives, but one variation of them, and its lesser forms are always available to aggressive government-corporate leaders seeking to maximize extractive potential (Baptist, 2014). In other words, as Cory Doctorow has provocatively argued, "Our networks have given the edge to the elites, and unless we seize the means of information, we are headed for a long age of [ICT]-powered feudalism, where property is the exclusive domain of the super-rich, where your surveillance-supercharged Internet of Things treats you as a tenant-farmer of your life, subject to a license agreement instead of a constitution" (Doctorow, 2015).

Fair distribution of the value arising out of the new data streams is critical. The work of being watched (Andrejevic, 2004) is not fairly compensated (Scholz, 2013). Acting as human information nodes in the urban network is becoming another civic and economic duty that smart city dwellers are expected to perform. As Jennifer Gabrys explains, "Monitoring and managing data in order to feed back information into urban systems are practices that become constitutive of citizenship. Citizenship transforms into citizen sensing, embodied through practices undertaken in response to (and communication with) computational environments and technologies" [48]. To the extent corporations derive commercial value from this data, there must be provisions for equitable benefit sharing (Lanier, 2011). Otherwise, persons as dividuals will merely multiply the power of others to exploit rhizomatic connections, by providing ever more data flowing on networks.

At present, smart city boosters are far too prone to assume that a *benevolent* intelligence animates the networks of sensors and control mechanisms they plan to install. The "core values, orientations, usually unspoken (even unconscious) assumptions and beliefs about how political and economic system should be structured and the roles that various actors can and should play," are part of what Jonathan Swarts calls a "neoliberal political-economic imaginary" [49]. The predictable result is a failure of imagination: a normative agenda either mired in slight refinements in existing patterns of objects and data, or free-floating utopianism about governance as a machine that would go of itself. We have sought to provide the critical foundation needed to articulate the smart city's emancipatory potential for all its residents, rather than the elite, (mostly) men behind the curtain of its sensory apparatus. It is against that democratic egalitarian goal — of fair benefit and burden sharing — that alleged "smartenings" of the city must be measured.

About the authors

Jathan Sadowski is a Ph.D. candidate in the "Human and Social Dimensions of Science and Technology," in the Consortium for Science, Policy & Outcomes at Arizona State University. His research mostly focuses on social theory/justice and political economy of information-communication technology. He is currently writing a dissertation on the socio-politics of "smart cities".
E-mail: Jathan [dot] Sadowski [at] asu [dot] edu

Frank Pasquale is a Professor of Law at University of Maryland's Francis King Carey School of Law. His research addresses the challenges posed to information law by rapidly changing technology, particularly in the health care, Internet, and finance industries. He recently published *The black box society: The secret algorithms that control money and information* (Harvard University Press, 2015), which develops a social theory of reputation, search, and finance.
E-mail: fpasquale [at] law [dot] umaryland [dot] edu

Acknowledgments

We thank anonymous reviewers for constructive comments that benefitted this paper, as well as Dave Guston, Ed Finn, and Thad Miller for commenting on an earlier draft. One author thanks Stephanie Vasko for her support and helpful discussions. The other author wishes to thank audiences at the Electronic Privacy Information Center, International Association of Privacy Professionals, Roskilde University, Harvard's Berkman Center, and Theorizing the Web for illuminating and critical responses to various scenarios of control presented in this piece. Any mistakes and misunderstandings that still remain are, of course, our own.

Notes

[1] We use the words "smart" and "smart city" in scare quotes throughout the introduction to draw attention to the way that thoroughly normative language has become part of the established

discourse about how we even call and refer to these technologies and initiatives. After all, who wants to be "dumb" or reject "smart" — the very discourse provides supporters an *a priori* advantage.

2. http://share.cisco.com/internet-of-things.html.

3. Sterling, 2014, loc. 68.

4. *Ibid.*

5. Shelton, *et al.*, 2015, p. 16.

6. Hollands, 2008, p. 307.

7. Kitchin, 2014, p. 6.

8. Greenfield, 2013, loc. 1274.

9. Hollands, 2015, p. 70.

10. Kitchin and Dodge, 2011, p. 131.

11. Geertz, 1973, p. 194.

12. Solum, 2014, p. 75.

13. *Ibid.*

14. *Ibid.*

15. Mirowski, 2013, p. 58.

16. http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=d3e33bde-30fd-4899-b30d-906b47e117ca&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a (11 February 2015), accessed 2 April 2015.

17. Goldsmith and Crawford, 2014, p. 6.

18. Goldsmith and Crawford, 2014, p. 112.

19. Goldsmith and Crawford, 2014, p. 4.

20. Cotterell, 2006, p. 15.

21. Foucault, 1990, p. 139, emphasis original.

22. Foucault, 1990, p. 136, emphasis original.

23. Gabrys, 2014, p. 32.

24. Habermas, 1996, p. 306.

25. Deleuze, 1995, pp. 181–182.

26. Langdon Winner (1977) provides several examples in the opening sections of *Autonomous technology*.

27. Mirowski, 2013, p. 77.

28. This concept functions as what Robert Merton (1968, p. 39) calls a "middle-range theory," which is intermediate to the "all-inclusive speculations" of "grand" social theories and the "minor working hypotheses" that are abundant in descriptive empirical research. Following from Merton, we find this level of theory to be appropriate to social theory, for it develops at the beneficial point of overlap between concrete fact and abstract theory.

29. Taylor, 1971, p. 3.

30. Peppet, 2011, p. 1,153.

31. Agamben, 2010, p. 43.

32. Graham, 2002, p. 238.

33. This discussion of biometrics is a modified and expanded version of Sadowski (2014b). We thank *Al Jazeera America* for allowing us to use parts of this article here.

[34] The transcript of this hearing — called “What information do data brokers have on consumers, and how do they use it?” — can be found at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=a47c081a-d653-4272-8d12-d6edc1e04dc6&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=12&YearDisplay=2013 (18 December 2013).

[35] Roderick, 2014, p. 740.

[36] Magnet, 2011, p. 12.

[37] Monahan, 2010, pp. 99–100.

[38] Graham, 2009; Virilio, 2005, p. 187.

[39] Virilio, 2009, p. 204.

[40] Shay, *et al.*, forthcoming: p. 4; McCoy, 2009.

[41] An article in *The Police Chief* magazine (Beck and McCue, 2009), co-authored by the Chief of Detectives for LAPD and the CEO of a security consultancy, asks: “Predictive policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession?” Hint: quite a lot, apparently.

[42] Graham, 2011, p. 121.

[43] Gandy, 2005, p. 28.

[44] Haraway, 1991, p. 163.

[45] Deleuze, 1995, pp. 174–175.

[46] Harvey, 2008, p. 23.

[47] Vanolo, 2014, p. 884.

[48] Gabrys, 2014, p. 34.

[49] Swarts, 2013, pp. 16–17.

References

G. Agamben, 2010. *Nudities*. Translated by D. Kishik and S. Pedatella. Stanford, Calif.: Stanford University Press.

M. Andrejevic, 2004. “The work of watching one another: Lateral surveillance, risk, and governance,” *Surveillance & Society*, volume 2, number 4, pp. 479–497, and at http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3359, accessed 26 June 2015.

J. Angwin, 2014. “Has privacy become a luxury good?” *New York Times* (3 March), at http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html, accessed 26 June 2015.

I. Arnsdorf, 2010. “The museum is watching you: Galleries quietly study what people like, or skip, to decide what hangs where,” *Wall Street Journal* (18 August), at http://www.wsj.com/articles/SB10001424052748704554104575435463594652730, accessed 26 June 2015.

A. Bady, 2013. “The MOOC moment and the end of reform,” *Liberal Education*, volume 99, number 4, pp. 6–15, and at http://thenewinquiry.com/blogs/zunguzungu/the-mooc-moment-and-the-end-of-reform/, accessed 26 June 2015.

E. Baptist, 2014. *The half has never been told: Slavery and the making of American capitalism*. New York: Basic Books.

R. Balko, 2013. *Rise of the warrior cop: The militarization of America’s police forces*. New York: PublicAffairs.

D. Baum, 2011. “The ultimate jam session: While Singapore succeeds with an iron fist, the United States waits for the invisible hand,” *Wired* (November), at http://archive.wired.com/wired/archive/9.11/singapore.html, accessed 26 June 2015.

K. Bobo, 2011. *Wage theft in America: Why millions of working Americans are not getting paid — and what we can do about it*. New York: New Press.

W. Bogard, 1996. *The simulation of surveillance: Hypercontrol in telematic societies*. New York: Cambridge University Press.

K. Campbell-Dollaghan, 2014. "Police are testing a 'live Google Earth' to watch crime as it happens," *Gizmodo* (14 April), at http://gizmodo.com/police-are-testing-a-live-google-earth-to-watch-crime-1563010340, accessed 26 June 2015.

D. Carpenter and D. Moss (editors), 2013. *Preventing regulatory capture: Special interest influence and how to limit it*. Cambridge: Cambridge University Press.

Castle Press, 2010. "Personicx life stage clusters," at https://www.castlepress.net/cp_assets/CP_Lifestyle.pdf, accessed 26 June 2015.

J. Chambers and W. Elfrink, 2014. "The future of cities: The Internet of everything will change how we live," *Foreign Affairs* (31 October), at http://www.foreignaffairs.com/articles/142324/john-chambers-and-wim-elfrink/the-future-of-cities, accessed 26 June 2015.

D.K. Citron and F. Pasquale, 2011. "Network accountability for the domestic intelligence apparatus," *Hastings Law Journal*, volume 62, number 1, pp. 1,441–1,494.

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

R. Cotterell, 2006. *Law, culture and society: Legal ideas in the mirror of social theory*. Hampshire: Ashgate.

J. Crary, 2013. *24/7: Late capitalism and the ends of sleep*. London: Verso.

G. Deleuze, 1995. *Negotiations, 1972–1990*. Translated by M. Joughin. New York: Columbia University Press.

Democracy now! 2011. "Police crackdowns on Occupy protests from Oakland to New York herald the 'new military urbanism'" (16 November), at http://www.democracynow.org/2011/11/16/police_crackdowns_on_occupy_protests_from, accessed 26 June 2015.

C. Doctorow, 2015. "Technology should be used to create social mobility — Not to spy on citizens," *Guardian* (10 March), at http://www.theguardian.com/technology/2015/mar/10/nsa-gchq-technology-create-social-mobility-spy-on-citizens, accessed 26 June 2015.

C. Doctorow, 2014. "Riot control drone that fires paintballs, pepper-spray and rubber bullets at protesters," *Boing Boing* (17 June), at http://boingboing.net/2014/06/17/riot-control-drone-that-paintb.html, accessed 26 June 2015.

M. Foucault, 1990. *The history of sexuality*. Volume 1: *An introduction*. Translated by R. Hurley. New York: Vintage.

N. Fraser, 1995. "From redistribution to recognition? Dilemmas of justice in a 'post-socialist' age," *New Left Review*, number 212, pp. 68–93.

C. Friedersdorf, 2014. "Eyes over Compton: How police spied on a whole city," *Atlantic* (21 April), at http://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/, accessed 26 June 2015.

J. Gabrys, 2014. "Programming environments: Environmentality and citizen sensing in the smart city," *Environment and Planning D: Society and Space*, volume 32, number 1, pp. 30–48.
doi: http://dx.doi.org/10.1068/d16812, accessed 26 June 2015.

M. Gandy, 2005. "Cyborg urbanization: Complexity and monstrosity in the contemporary city," *International Journal of Urban and Regional Research*, volume 29, number 1, pp. 26–49.
doi: http://dx.doi.org/10.1111/j.1468-2427.2005.00568.x, accessed 26 June 2015.

C. Geertz, 1973. *The interpretation of cultures: Selected essays*. New York: Basic Books.

T.F. Gieryn, 2006. "City as truth-spot: Laboratories and field-sites in urban studies," *Social Studies of Science*, volume 36, number 1, pp. 5–38.
doi: http://dx.doi.org/10.1177/0306312705054526, accessed 26 June 2015.

S. Goldsmith and S. Crawford, 2014. *The responsive city: Engaging communities through data-smart governance*. San Francisco: Jossey-Bass.

S. Graham, 2011. *Cities under siege: The new military urbanism*. London: Verso.

S. Graham, 2009. "The urban 'battlespace'," *Theory, Culture & Society*, volume 26, numbers 7–8, pp. 278–288.
doi: http://dx.doi.org/10.1177/0263276409349280, accessed 26 June 2015.

S. Graham, 2002. "CCTV: The stealthy emergence of a fifth utility?" *Planning Theory & Practice*, volume 3, number 2, pp. 237–241.
doi: http://dx.doi.org/10.1080/14649350220150116, accessed 26 June 2015.

A. Greenfield, 2013. *Against the smart city*. New York: Do Projects.

J. Habermas, 1996. *Between facts and norms: Contributions to a discourse theory of law and democracy*. Translated by W. Rehg. Cambridge, Mass.: MIT Press.

J. Habermas, 1984. *The theory of communicative action*. Volume 1: *Reason and the rationalization of society*. Translated by T. McCarthy. Boston, Mass.: Beacon Press.

O. Halpern, J. LeCavalier, N. Calvillo, and W. Pietsch, 2013. "Test-bed urbanism," *Public Culture*, volume 25, number 2, pp. 273–306.
doi: http://dx.doi.org/10.1215/08992363-2020602, accessed 26 June 2015.

D. Haraway, 1991. "A cyborg manifesto: Science, technology, and socialist-feminism in the late twentieth century," In: D. Haraway. *Simians, cyborgs, and women: The reinvention of nature*. New York: Routledge, pp. 149–181.

B. Harcourt, 2012. "Political disobedience," *Critical Inquiry*, volume 39, number 1, pp. 33–55.
doi: http://dx.doi.org/10.1086/668049, accessed 26 June 2015.

D. Harvey, 2008. "The right to the city," *New Left Review*, number 53, pp. 23–40, and at http://newleftreview.org/II/53/david-harvey-the-right-to-the-city, accessed 29 June 2015.

D. Harvey, 1989. "From managerialism to entrepreneurialism: The transformation in urban governance in late capitalism," *Geografiska Annaler. Series B, Human Geography*, volume 71, number 1, pp. 3–17.
doi: http://dx.doi.org/10.2307/490503, accessed 26 June 2015.

R.G. Hollands, 2015. "Critical interventions into the corporate smart city," *Cambridge Journal of Regions, Economy and Society* volume 8, number 1, pp. 61–77.
doi: http://dx.doi.org/10.1093/cjres/rsu011, accessed 26 June 2015.

R.G. Hollands, 2008. "Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?" *City*, volume 12, number 3, pp. 303–320.
doi: http://dx.doi.org/10.1080/13604810802479126, accessed 26 June 2015.

C.J. Hoofnagle, 2003. "Big brother's little helpers: How Choicepoint and other commercial data brokers collect and package your data for law enforcement," *North Carolina Journal of International Law & Commercial Regulation*, volume 29, number 1, pp. 595–637, and at https://www.law.unc.edu/journals/ncilj/issues/volume29/number-4-summer-2003/big-brothers-little-helpers-how-choicepoint-and-other-commercial-data-brokers-collect-and-package-your-data-for-law-enforcement/, accessed 26 June 2015.

N. Jurgenson, 2012. "When atoms meet bits: Social media, the mobile Web and augmented revolution," *Future Internet*, volume 4, number 1, pp. 83–91.
doi: http://dx.doi.org/10.3390/fi4010083, accessed 26 June 2015.

R. Kitchin, 2014. "The real-time city: Big data and smart urbanism," *GeoJournal*, volume 79, number 1, pp. 1–14.
doi: http://dx.doi.org/10.1007/s10708-013-9516-8, accessed 26 June 2015.

R. Kitchin and M. Dodge, 2011. *Code/space: Software and everyday life*. Cambridge, Mass.: MIT Press.

N. Krieger, 1994. "Epidemiology and the web of causation: Has anyone seen the spider?" *Social Science & Medicine*, volume 39, number 7, pp. 887–903.
doi: http://dx.doi.org/10.1016/0277-9536(94)90202-X, accessed 26 June 2015.

J. Lanier, 2011. *You are not a gadget: A manifesto*. New York: Vintage.

L. Lessig, 1999. *Code and other laws of cyberspace*. New York: Basic Books.

C. Lévi-Strauss, 1966. *The savage mind*. Chicago: University of Chicago Press.

S.A. Magnet, 2011. *When biometrics fail: Gender, race, and the technology of identity*. Durham, N.C.: Duke University Press.

J. Manzi, 2012. *Uncontrolled: The surprising payoff of trial-and-error for business, politics, and society*. New York: Basic Books.

A.W. McCoy, 2009. "Welcome home, war! How America's wars are systematically destroying our liberties," *TomDispatch* (12 November), at http://www.tomdispatch.com/blog/175154/tomgram%3A_alfred_mccoy,_surveillance_state,_u.s.a., accessed 26 June 2015.

R.K. Merton, 1968. "On sociological theories of the middle range," In: R.K. Merton. *Social theory and social structure*. Enlarged edition. New York: Free Press, pp. 39–53.

P. Mirowski, 2013. *Never let a serious crisis go to waste: How neoliberalism survived the financial meltdown*. London: Verso.

T. Monahan, 2010. "Surveillance as governance: Social inequality and the pursuit of democratic surveillance," In: K.D. Haggerty and M. Samatas (editors). *Surveillance and democracy*. New York: Routledge, pp. 91–110.

E. Morozov, 2014. "Every little byte counts," *New York Times* (16 May), at http://www.nytimes.com/2014/05/18/books/review/the-naked-future-and-social-physics.html, accessed 26 June 2015.

P. Neirotti, A. De Marco, A.C. Cagliano, G. Mangano, F. Scorrano, 2014. "Current trends in smart city initiatives: Some stylised facts," *Cities*, volume 38, pp. 25–36.
doi: http://dx.doi.org/10.1016/j.cities.2013.12.010, accessed 26 June 2015.

G. Newsom, 2013. *Citizenville: How to take the town square digital and reinvent government*. New York: Penguin.

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

S. Palmisano, 2010. "Building a smarter planet: The time to act is now," speech given at Chatham House, London (12 January), at http://www.ibm.com/smarterplanet/us/en/events/sustainable_development/12jan2010/, accessed 26 June 2015.

S. Peppet, 2011. "Unraveling privacy: The personal prospectus and the threat of a full disclosure future," *Northwestern University Law Review*, volume 105, number 3, pp. 1,153–1,204, and at http://www.northwesternlawreview.org/issues/105/3, accessed 26 June 2015.

M. Purcell, 2002. "Excavating Lefebvre: The right to the city and its urban politics of the inhabitant," *GeoJournal*, volume 58, numbers 2–3, pp. 99–108.
doi: http://dx.doi.org/10.1023/B:GEJO.0000010829.62237.8f, accessed 26 June 2015.

Reuters, 2015. "IBM says to invest $3 billion in 'Internet of things' unit" (31 March), at http://www.reuters.com/article/2015/03/31/us-ibm-investment-idUSKBN0MR0BS20150331, accessed 26 June 2015.

L. Roderick, 2014. "Discipline and power in the digital age: The case of the US consumer data broker industry," *Critical Sociology* volume 40, number 5, pp. 729–746.
doi: http://dx.doi.org/10.1177/0896920513501350, accessed 26 June 2015.

C. Rosen, 2012. "The machine and the ghost," *New Republic* (12 July), at http://www.newrepublic.com/article/books-and-arts/magazine/104874/rosen-verbeek-technology-morality-intelligence, accessed 26 June 2015.

D. Rothkopf, 2009. *Superclass: The global power elite and the world they are making*. New York: Farrar, Straus and Giroux.

J. Sadowski, 2014a. "Insurance vultures and the Internet of things," *Baffler* (11 June), at http://www.thebaffler.com/blog/insurance-vultures-and-the-internet-of-things/, accessed 26 June 2015.

J. Sadowski, 2014b. "Biometrics are coming for you," *Al Jazeera America* (6 July), at http://america.aljazeera.com/opinions/2014/7/biometrics-big-datamining.html, accessed 26 June 2015.

J. Sadowski and F. Pasquale, 2014. "Creditors use new devices to put squeeze on debtors," *Al-Jazeera America* (9 November), at http://america.aljazeera.com/opinions/2014/11/debt-collectiontechnologystarterinterruptdevicesubprime.html, accessed 26 June 2015.

J. Sadowski and E. Selinger, 2014. "Creating a taxonomic tool for technocracy and applying it to Silicon Valley," *Technology in Society*, volume 38, pp. 161–168. doi: http://dx.doi.org/10.1016/j.techsoc.2014.05.001, accessed 26 June 2015.

B. Salinas, 2013. "High-end stores use facial recognition tools to spot VIPs," *NPR All Tech Considered* (21 July), at http://www.npr.org/blogs/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips, accessed 26 June 2015.

R. Santus, 2014. "Hackers claim they can copy fingerprints from photos," *Mashable* (29 December), at http://mashable.com/2014/12/29/fingerprint-photo-copy/, accessed 26 June 2015.

B. Schneier, 2014. "The Internet of things is wildly insecure — and often unpatchable," *Schneier on Security* (6 January), at https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html, accessed 26 June 2015.

T. Scholz (editor), 2013. *Digital labor: The Internet as playground and factory*. New York: Routledge.

L. Shay, W. Hartzog, J. Nelson, D. Larkin, andG. Conti, forthcoming. "Confronting automated law enforcement," In: R. Calo, M. Froomkin, and I. Kerr (editors). *Robot law*. Northampton, Mass.: Edward Elgar; version at http://robots.law.miami.edu/wp-content/uploads/2012/01/Shay-EtAl-ConfrontingAutomatedLawEnf.pdf, accessed 26 June 2015.

T. Shelton, M. Zook, and A. Wiig, 2014. "The 'actually existing smart city'," *Cambridge Journal of Regions, Economy and Society*, volume 8, number 1, 13–25. doi: http://dx.doi.org/10.1093/cjres/rsu026, accessed 26 June 2015.

O. Söderström, T. Paasche, and F. Klauser, 2014. "Smart cities as corporate storytelling," *City*, volume 18, number 3, pp. 307–320. doi: http://dx.doi.org/10.1080/13604813.2014.906716, accessed 26 June 2015.

L. Solum, 2014. "Artificial meaning," *Washington Law Review*, volume 89, number 1, pp. 69–86, and at https://www.law.uw.edu/wlr/print-edition/past-issues/vol-89/1/artificial-meaning/, accessed 26 June 2015.

S.L. Star, 1999. "The ethnography of infrastructure," *American Behavioral Scientist*, volume 43, number 3, pp. 377–391. doi: http://dx.doi.org/10.1177/00027649921955326, accessed 26 June 2015.

B. Sterling, 2014. *The epic struggle of the Internet of things*. Moscow: Strelka Press.

J. Swarts, 2013. *Constructing neoliberalism: Economic transformation in Anglo-American democracies*. Toronto: University of Toronto Press.

C. Taylor, 1971. "Interpretation and the sciences of man," *Review of Metaphysics*, volume 25, number 1, pp. 3–51.

A.M. Townsend, 2014. *Smart cities: Big data, civic hackers, and the quest for a new utopia*. New York: Norton.

R. Unger, 2004. *Plasticity into power: Comparative-historical studies on the institutional conditions of economic and military success*. London: Verso.

U.K. Department For Business, Innovation & Skills, 2013. "The smart city market: opportunities for the UK," *BIS Research Paper* 136 (October), at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217-smart-city-market-opportunties-uk.pdf, accessed 26 June 2015.

A. Vanolo, 2014. "Smartmentality: The smart city as disciplinary strategy," *Urban Studies*, volume 51, number 5, pp. 883–898. doi: http://dx.doi.org/10.1177/0042098013494427, accessed 26 June 2015.

R. Verchick, 2010. *Facing catastrophe: Environmental action for a post-Katrina world*. Cambridge, Mass.: Harvard University Press.

P. Virilio, 2005. *Negative horizon: An essay in dromoscopy*. New York: Continuum.

P. Virilio, 2009. "The state of emergency," In: H. Rosa and W. Scheuerman (editors). *High-speed society: Social acceleration, power, and modernity*. University Park, Pa.: Pennsylvania State University Press, pp. 201–214.

S. Walker and O. Grytsenko, 2014. "Text messages warn Ukraine protesters they are 'participants in mass riot'," *Guardian* (21 January), at http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot, accessed 26 June 2015.

B. Wasik, 2013. "In the programmable world, all our objects will act as one," *Wired* (14 May), at http://www.wired.com/2013/05/internet-of-things-2/all/, accessed 30 October 2014.

L. Wacquant, 2008. "The militarization of urban marginality: Lessons from the Brazilian metropolis," *International Political Sociology*, volume 2, number 1, pp. 56–74.
doi: http://dx.doi.org/10.1111/j.1749-5687.2008.00037.x, accessed 26 June 2015.

L. Winner, 1977. *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, Mass.: MIT Press.

J. Winters, 2011. *Oligarchy*. New York: Cambridge University Press.

Editorial history

Received 12 March 2015; revised 22 May 2015; accepted 23 June 2015.

The spectrum of control: A social theory of the smart city
by Jathan Sadowski and Frank Pasquale.
First Monday, Volume 20, Number 7 - 6 July 2015
http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/5903/4660
doi: http://dx.doi.org/10.5210/fm.v20i7.5903