



DOROTHY H. HOOVER LIBRARY
Course Reserves

Greenfield, Adam. "The Internet of Things: A Planetary Mesh of Perception and Response." *Radical Technologies: The Design of Everyday Life*, Verso, 2018, pp. 31-62.

Copied under Permission from Access Copyright. Further reproduction, distribution or transmission is prohibited, except as otherwise permitted by law.

The internet of things

A planetary mesh of perception and response

In Copenhagen, a bus running two minutes behind schedule transmits its location and passenger count to the municipal traffic signal network, which extends the green light at each of the next three intersections long enough for its driver to make up some time. In Davao City in the Philippines, an unsecured webcam overlooks the storeroom of a fast-food stand, allowing anyone equipped with its address to peer in at will on all its comings and goings. In San Francisco, a young engineer hopes to “optimize” his life through sensors that track his heart rate, respiration and sleep cycle.

What links these wildly different circumstances is a vision of connected devices now being sold to us as the “internet of things,” in which a weave of networked perception wraps every space, every place, every thing and every body on Earth. The technologist Mike Kuniavsky, a pioneer and early proponent of this vision, characterizes it as a state of being in which “computation and data communication [are] embedded in, and

distributed through, our entire environment.”¹ I prefer to see it for what it is: the colonization of everyday life by information processing.

Like the smartphone, the internet of things isn’t a single technology, but an unruly assemblage of protocols, sensing regimes, capabilities and desires, all swept under a single rubric for the sake of disciplinary convenience. Just about all that connects the various devices, services, vendors and efforts involved is the ambition to raise awareness of some everyday circumstance to the network for analysis and response.

Though it can often feel as if this colonization proceeds of its own momentum, without any obvious driver or particularly pressing justification beyond the fact that it is something our technology now makes possible, it always pays to remember that distinct ambitions are being served wherever and however the internet of things appears, whether as rhetoric or reality. Some of these ambitions speak to the needs of commercial differentiation, and the desire to instill the qualities of surprise and delight into otherwise banal products. Others are founded in a much more concrete and pragmatic set of concerns, having to do with the regulation of energy consumption or the management of municipal infrastructure. Inevitably, some of these ambitions involve surveillance, security and control. But whatever the context in which these connected devices appear, what unites them is the inchoate terror that a single event anywhere might be allowed to transpire unobserved, uncaptured and unleveraged.

This, then, is the internet of things. If the endeavor retains a certain sprawling and formless quality, we can get a far more concrete sense of what it involves, what it invokes and what it requires by looking at each of the primary scales at which it appears to us: that of the body, that of the room, and that of public space in general. Though they all partake of the same general repertoire of techniques, each of these domains of activity has a specific, distinguishing label associated with it. The quest to instrument the body, monitor its behavior and derive actionable insight from these soundings is known as the

“quantified self”; the drive to render interior, domestic spaces visible to the network “the smart home”; and when this effort is extended to municipal scale, it is known as “the smart city.” Each of these scales of activity illuminates a different aspect of the challenge presented to us by the internet of things, and each of them has something distinct to teach us.

At the most intimate scale, the internet of things manifests in the form of wearable biometric sensors: devices that collect the various traces of our being in the world, and submit them to the network for inspection and analysis. The simplest of these are little more than networked digital pedometers. Using the same kind of microelectromechanical accelerometer found in our smartphones, these count steps, measure overall distance traversed, and furnish an estimate of the calories burned in the course of this activity. More elaborate models measure heart rate, breathing, skin temperature and even perspiration—biological primitives from which higher-order, harder-to-define psychoemotional states like stress, boredom or arousal can be inferred.

We can understand these devices as hinges between the body and the network: ways of raising the body’s own processes directly to the network, where they can be stored or mined for insight like any other data set. These latent indicators of biological performance, otherwise so hard to discern, are made legible in order that they may be rendered subject to the exercise of will, and brought under at least some semblance of control.

While the various models of Fitbit are probably the most widely used wearable biometric monitors, the Apple Watch is currently the most polished example of the category—indeed, lower-than-anticipated sales when initially marketed as a fashion accessory have spurred Apple to reposition its offering as a high-performance fitness device. With its obsessively detailed design, precision machining and luxury-grade materials, the Watch looks and feels a good deal less “technical” than its competitors. But it is every bit as capable of harvesting biometric data across multiple regimes, if not more so, and its colorful

visualizations, trend lines and insistent reminders incorporate the latest findings of motivational psychology. It may be the long-awaited breakthrough in wearables: both the enabler and the visible symbol of a lifestyle in which performance is continuously monitored and plumbed for its insights into further improvements.

Nobody has embraced this conception of instrumented living more fervently than a loose global network of enthusiasts called the Quantified Self, whose slogan is “self-knowledge through numbers.”² Founded by *Wired* editor Gary Wolf and *Whole Earth Review* veteran Kevin Kelly in 2007, the Quantified Self currently boasts a hundred or so local chapters, and an online forum where members discuss and rate the devices mobilized in their self-measurement efforts. (It can be difficult to disentangle this broader movement from a California company of the same name also founded by Wolf and Kelly, which mounts conferences dedicated to proselytizing for the practice of self-measurement.)

In their meetups and on their forum, the stalwarts of the Quantified Self discuss the theory and practice of the measured life, mulling everything from the devices most effective at capturing REM sleep to the legalities involved in sharing data. One forum thread goes quite a bit further; entitled “Can You Quantify Inner Peace?,” it discusses metrics that the instrumented aspirant might use to measure their progress toward heights of consciousness previously understood as the preserve of Zen meditators and yogic adepts.

As an individual lifestyle choice, none of this is properly anyone else’s to question, and there’s no doubt that the effort can occasionally yield up some provocative insights. Consider the young cognitive neuroscientist who cross-referenced her online purchases, entertainment choices and dating decisions against her menstrual cycle,³ and found among other things that she only ever purchased red clothing when she was at her most fertile.

What almost never seems to be addressed in these forums and meetups, though, are questions about what this self-knowledge

is being mobilized for, and just where the criteria against which adherents feel they need to optimize their performance come from in the first place. While there are some fascinating questions being explored in the Quantified Self community, a brutal regime of efficiency operates in the background. Against the backdrop of late capitalism, the rise of wearable biometric monitoring can only be understood as a disciplinary power traversing the body itself and all its flows. This is a power that Frederick Taylor never dreamed of, and Foucault would have been laughed out of town for daring to propose.

It's clear that the appeal of this is overwhelmingly to young workers in the technology industry itself, the control they harvest from the act of quantification intended to render them psychophysically suitable for performance in a work environment characterized by implacable release schedules and a high operational tempo. (Not for nothing is there a very significant degree of overlap between the Quantified Self and the "lifehacking" subculture—the same people who brought you Soylent⁴, the flavorless nutrient slurry that is engineered to be a time-and-effort-efficient alternative to actual meals.) And of course what is most shocking about all of this is that it is undertaken voluntarily. Here, a not-insignificant percentage of the population has so decisively internalized the values of the market for their labor that the act of resculpting themselves to better meet its needs feels like authentic self-expression. They are willing to do whatever it takes to reengineer the body so it gets more done in less time, is easier and more pleasant to work with—to render themselves, as the old Radiohead lyrics put it, "calm, fitter, healthier and more productive," and in so doing transform themselves into all-but-fungible production units, valued only in terms of what they offer the economy.

What may be unproblematic as the niche interest of a technical subculture becomes considerably more worrisome when its tenets are normalized as a way of life appropriate for the rest of us. But it is of yet greater concern when it becomes mandated by actors that operate at societal scale, and have the leverage to impose these choices upon us.

For now, this takes the form of a carrot: health insurance companies, including Aetna in the United States and Vitality in the United Kingdom,⁵ have already extended their customers steep discounts on the Apple Watch, and offer reduced premiums for those whose Watches continue to report a high and regular level of exercise. But it isn't hard to see how this way of eliciting compliance could easily be transformed into a stick, with punitively higher rates—or even the refusal of coverage altogether—for those customers unwilling to share these most intimate facts of the body over the global network.

If these practices of the Quantified Self ever do spur any one individual to genuine introspection, impelling them to reckon with the true nature of their self as it manifests in this body and this life, then so much the better. But the Delphic injunction to “know thyself” hardly seems honored in the decision to strap on a Fitbit. And whatever gains may accrue to the occasional individual, they pale in comparison with everything that is sure to be lost when the posture of the body and all the details of its situation in space and time are used collectively, to construct models of nominal behavior we're all thereafter forced to comply with.

If wearable biometric devices are aimed, however imperfectly, at rigorous self-mastery, the colonization of the domestic environment by similarly networked products and services is intended to deliver a very different experience: convenience. The clear aim of such “smart home” efforts is to as nearly as possible short-circuit the process of reflection that stands between one's recognition of a desire and its fulfillment via the market.

The apotheosis of this tendency is a device currently being sold by Amazon, the Dash Button. Many internet-of-things propositions are little more than some more or less conventional object with networked connectivity tacked on, and their designers have clearly struggled to imagine what that connectivity could possibly be used for. The Dash Button is the precise opposite, a thing in the world that could not possibly have existed without the internet—and not merely some abstract network of networks, but the actual internet we have, populated by the precise mix

of devices and services the more privileged among us habitually call upon in the course of their lives. I cannot possibly improve on Amazon's own description of this curious object and how it works, so I'll repeat it in full here:

Amazon Dash Button is a Wi-Fi connected device that reorders your favorite item with the press of a button. To use Dash Button, simply download the Amazon App from the Apple App Store or Google Play Store. Then, sign into your Amazon Prime account, connect Dash Button to Wi-Fi, and select the product you want to reorder. Once connected, a single press on Dash Button automatically places your order. Amazon will send an order confirmation to your phone, so it's easy to cancel if you change your mind. Also, the Dash Button Order Protection doesn't allow a new order to be placed until the prior order ships, unless you allow multiple orders.⁶

So: a branded, single-purpose electronic device, and quite an elaborate one at that, whose entire value proposition is that you press it when you're running out of detergent, or toilet paper, or coffee beans, and it automatically composes an order request to Amazon. I don't for a second want to downplay the value of a product like this for people who have parents to look after, or kids to drop off at daycare, or who live amid social and spatial conditions where simply getting in the car to go pick up some laundry detergent may take an hour or more out of their day. But the benefit is sharply differential. You get your detergent on time, yes, but Amazon gets so much more. They get data on the time and place of your need, as well as its frequency and intensity, and that data has value. It is, explicitly, an asset, and you can be sure they will exploit that asset in every way their terms and conditions permit them to—including by using it to develop behavioral models that map the terrain of our desires, so as to exploit them with even greater efficiency in the future.

Again, the aim of devices like the Dash Button is to permit the user to accomplish commercial transactions as nearly as possible without the intercession of conscious thought, even the

few moments of thought involved in tapping out commands on the touchscreen of a phone or tablet. The data on what the industry calls “conversion” is as clear as it is unremitting: for every box to tick, form to fill or question that needs to be answered, the percentage of remaining users that makes it all the way to checkout tumbles.

For the backers of commercial internet-of-things ventures, this falloff is the stuff of sleepless nights and sour stomachs. And yet manufacturers, enticed by the revenue potential inherent in a successful conquest of the domestic environment, keep trying, in the hope that sooner or later one of the connected products and services on offer will be embraced as something as essential to everyday life as the smartphone. We can understand the recent industry push toward the “smart home” as simply the latest version of this: a conscious, coherent effort to enlist our intimate spaces as a site of continuous technological upgrade, subscription-based services and the perpetual resupply of consumables. Perhaps the promise of effortless convenience can succeed in convincing consumers to sign on, where the sheer novelty of being connected did not.

For the moment, this strategy has come to center on so-called smart speakers, a first generation of which have now reached the market—products like the Amazon Echo and Google Home, each of which is supposed to function as a digital hub for the home. As we might by now expect of networked things, nothing about the physical form of these objects goes any way at all toward conveying their purpose or intended mode of function: Amazon’s Echo is a simple cylinder, and its Echo Dot that same cylinder hacked down to a puck, while the Google Home presents as a beveled ovoid. The material form of such speakers is all but irrelevant, though, as their primary job is to function as the physical presence of and portal onto a service—specifically, a branded “virtual assistant.”

Google, Microsoft, Amazon and Apple each offer their own such assistant, based on natural-language speech recognition; no doubt further competitors and market entrants will have appeared by the time this book sees print. Almost without

exception, these assistants are given female names, voices and personalities, presumably based on research conducted in North America indicating that users of all genders prefer to interact with women.⁷ Apple's is called Siri, Amazon's Alexa; Microsoft, in dubbing their agent Cortana, has curiously chosen to invoke a character from their *Halo* series of games, polluting that universe without seeming to garner much in return. For now, at least, Google has taken a different tack, refreshingly choosing not to give their assistant offering any token of gendered personal identity, even in the rudimentary form of a name.⁸ One simply addresses it as "Google."

Gendered or otherwise, these assistants live in a smart speaker the way a genie might in its bottle, from where they are supposed to serve as the command hub of a connected home. The assistant furnishes an accessible, easy-to-use front end on what might otherwise be an overwhelming number of controls scattered in different places throughout the home, subsuming those for lighting and entertainment, security functions, and heating, cooling and ventilation systems; through a selection of APIs, it also reaches out to engage third-party commercial services. Whether or not this scenario appeals to a significant audience, or corresponds to the way in which anyone actually lives, it is of powerful interest to the manufacturers, who in this way establish a beachhead in the home for the brand—a point of presence, and a means of considerable leverage.

At first blush, devices like these seem harmless enough. They sit patiently in the periphery of attention, never pressing any kind of overt claim on their users, and are addressed in the most natural way imaginable: conversationally. But the details of implementation shed some light on just what this is all for. This is how Google's assistant works: you mention to it that you're in the mood for Italian, and it "will then respond with some suggestions for tables to reserve at Italian restaurants using, for example, the OpenTable app."⁹ This scenario was most likely offered off the top of the head of the journalist who wrote it. But it's instructive, a note-perfect illustration of the principle that though the choices these assistants offer us are presented

as neutral, they invariably arrive prefiltered through existing assumptions about what is normal, what is valuable, and what is appropriate. Their ability to channel a nascent, barely articulated desire into certain highly predictable kinds of outcomes bears some scrutiny.

Ask restaurateurs and front-of-house workers what they think of OpenTable, for example, and you'll swiftly learn that one person's convenience is another's accelerated work tempo, or worse. You'll learn that restaurants offering reservations via the service are "required to use the company's proprietary floor management system, which means leasing hardware and using OpenTable-specific software," and that OpenTable retains ownership of all the data generated in this way.¹⁰ You'll also learn that OpenTable takes a cut on reservations made of one dollar per seated diner, which obviously adds up to a very significant amount on a busy night. Conscientious diners (particularly those with some experience working in the industry) have therefore been known to bypass the ostensible convenience of OpenTable, and make whatever reservations they have to by phone. By contrast, Google Home's all but frictionless default to making reservations via OpenTable normalizes that option, the same way the appearance of Uber as a default option in the Google Maps interface sanctifies the choice to use that service.

This is hardly accidental. It reflects the largely preconscious valuations, priorities and internalized beliefs of the people who devised Home—at Google, as throughout the industry, a remarkably homogeneous cohort of young designers and engineers, still more similar to one another psychographically and in terms of their political commitments than they are demographically alike.¹¹ But as with those who have embraced the practices of the Quantified Self, what is more important than the degree of similarity they bear to one another is how different they are from everyone else.

I don't think it's unfair to say that at this moment in history, internet-of-things propositions are generally imagined, designed and architected by a group of people who have completely assimilated services like Uber, Airbnb and Venmo into their daily

lives, at a time when Pew Research Center figures suggest that a very significant percentage of the population has never used (or even heard of) them.¹² And all of their valuations get folded into the things they design. These propositions are normal to them, and so become normalized for everyone else as well.

There are other challenges presented by this way of interacting with networked information. It's difficult, for example, for a user to determine whether the options they're being offered by a virtual assistant result from what the industry calls an "organic" return—something that legitimately came up in the result of a search process—or from paid placement. But the main problem with the virtual assistant is that it fosters an approach to the world that is literally thoughtless, leaving users disinclined to sit out any particularly prolonged frustration of desire, and ever less critical about the processes that result in the satisfaction of their needs and wants.

Whatever artifact they happen to be embedded in at any given moment, virtual assistants are literally listening to us at all times, and to everything that is said in their presence. But then, of course they are: as voice-activated interfaces, they must by definition be constantly attentive in this way, in order to detect when the "wake word" rousing them to action is spoken. That they are in this way enabled to harvest data that might be used to refine targeted advertising, or for other commercial purposes, is something that is only disclosed deep in the terms and conditions that govern their use.¹³ The logic operating here is that of preemptive capture: the notion that as a service provider you might as well trawl up everything you can, because you never know what value might be derived from it in the future.

This leads to situations that might be comical, were they not so very on-the-nose in what they imply about the networking of our domestic environments. These stories circulate in the internet of things community as cautionary tales; one of the best-known concerns the time the National Public Radio network aired a story about the Echo, and various cues spoken aloud on the broadcast were interpreted as commands by Echos belonging to members of the audience. (One listener reported

that just such a command had caused his Echo to reset the thermostat it was connected with to a balmy, and expensive, 70 degrees.)¹⁴

Here we see something that was intended as a strategy for the reduction of cognitive overload threatening to become one of its main drivers. What the designers of these experiences failed to imagine was that while an calming experience of use might have been narrowly achievable in a research lab, where total control might be imposed on every artifact and service operating in the local environment, it is virtually impossible to realize in a home where the things at play come from any number of vendors, with each interactive object in the space most likely designed from the tacit assumption that it would be the only one with a claim on anyone's attention.

Put to the side for one moment the question of disproportionate benefit—the idea that you as the user derive a little convenience from your embrace of a virtual assistant, while its provider gets *everything*, all the data and all the value latent in it. Let's simply consider what gets effaced in the ideology of ease¹⁵ that underlies this conception of the internet of things, this insistence that all tasks be made as simple as possible, at all times. Are the constraints presented to us by life in the non-connected world *really* so onerous? Is it really so difficult to wait until you get home to pre-heat the oven? And is it worth trading away so much, just to be able to do so remotely?

Like the Dash Button, connected products that are intended for consumers generally make great emphasis on their “plug-and-play” quality: a simplicity in use so refined that one might bring a product home, turn it on for the first time and step back as it autoconfigures itself. In emphasizing the appeal of this, manufacturers have correctly intuited that most people have neither the time, the knowledge nor the inclination to manage the details of a device’s connection with the internet. But the push toward ease often effaces something critical, and one of the things that all too frequently gets elided in the logic of plug-and-play is any consideration for network security.

This is especially the case where networked cameras are concerned. A cheap plug-and-play webcam, the kind of marginally adequate Shenzhen product you can currently pick up for around \$10, broadcasts to the internet in just the same way that an industrial-grade model costing ten or fifteen times as much would. But unlike that more considered product, it will lack even the most rudimentary means of controlling access to its feed. And this in turn means that when you use a specialized internet of things search engine like Shodan to seek out devices that are broadcasting unsecured, you turn up hundreds of thousands of them, located all over the planet.

Such feeds can be discovered by anyone with a mind to, and they open onto scenes you'd imagine people would treat with far greater discretion: illegal marijuana grow ops, secure areas of bank branches, military base housing, and column after column of babies lying in their cribs, asleep or otherwise.¹⁶ The sense of boundary transgression is intense. As I write these words, I have a tab open with a view onto what looks like the stock room of a Jollibee fast-food restaurant in Davao City in the Philippines; I wonder how the two young women on camera would react if they realized that their movements and actions were fully visible, albeit in low resolution, to a writer watching them from 7,300 miles away. Even cameras that do technically offer more elaborate security provisions are often left vulnerable as a consequence of that most human and persistent of blunders, the failure to change the default password that a device ships with. A search site based in Russia compiles links to some 73,000 cameras mounted in locations around the world, both outdoor and indoor, that are left unsecured in just this way.¹⁷

This tendency toward laziness is near-universal throughout the internet of things world, and beyond cameras it afflicts just about any class of objects that can be connected to the network. A security researcher named Matthew Garrett described his March 2016 stay in a London hotel,¹⁸ for example, where the guest-room light switches had been replaced with touchscreen Android tablets, presumably in the misguided pursuit of contemporary cool. With a few minutes' work, Garrett was able

to determine not only that the heating, cooling, lighting and entertainment controls for his room faced the global network unsecured, but that the last four digits of the IP address for every room in the hotel transparently mapped onto floor and room number. A digital intruder could take control of any room they desired to, at will—whether from the room next door, or from halfway around the world—simply by substituting the relevant digits in the IP address.

Every networked device that goes unprotected in this way isn't simply exposing its own controls. It can be suborned as a point of access to the entire local network and every other device connected to it,¹⁹ offering intruders an aperture through which they might install backdoors, intercept traffic passing across the network, or launch denial-of-service attacks.²⁰

My concern here isn't so much to point out that the internet of things is a security nightmare, although it certainly is. What I want to emphasize is that, in very large part, this is a direct consequence of commercial decisions, and a problem of business model. It's not all that expensive to furnish networked devices with security elaborate enough to defeat the more obvious exploits—but at the low end of the market, where profit margins are reed-thin, any additional increment of cost is intolerable. Similarly, the hotel with the Android-tablet light switches wanted bragging rights to an cutting-edge guest experience, but evidently wasn't prepared to invest in an effective security plan, or an addressing scheme that might prevent the controls in each room from being trivially guessed.

This is the open secret of the internet of things—each instance of which is, by definition, coupled to the same internet that carries by far the greater share of our civilization's communications, news, entertainment, and financial traffic. The price of connection is vulnerability, always and in every context, and it is no different here: every single device that is connected to the network offers an aperture, a way in, what the security community calls an “attack vector.” Taken together, these trillion unpatched vulnerabilities raise the specter of swarms of zombie machines directed to spam the internet infrastructure, and overwhelm it

with spurious traffic to the point that no legitimate message can get through. This is known as a “distributed denial of service” attack, or DDoS, and while it’s by no means sophisticated, it can be devastatingly effective.

If ever there were a situation in which a little bit of paranoia might be advisable, it’s this one. Understand, too, that the overwhelming majority of such vulnerabilities will never be patched. As internet security legend Bruce Schneier argues, the parties that understand the vulnerabilities—device manufacturers—aren’t incentivized to fix them, while the end user doesn’t have the expertise to do so.²¹

The reigning internet security paradigm was developed in an age where almost all networked devices were operated by institutions with full-fledged IT departments. The security conventions we rely on are predicated on the assumption that knowledgeable staff would always be available to patch vulnerabilities and ensure that firmware remained current. By contrast, the internet of things business model consists precisely in selling devices too cheap to have functional security provisions, to people who don’t know what firmware is or why it might present a vulnerability.

Every time someone buys a low-end device of this type off a pallet at Costco or PCWorld, takes it home and plugs it in, they expand the property of their local network that security professionals call its “attack surface,” or the total scope of exposure it presents to the world. And until someone manages to develop a security paradigm appropriate to these circumstances, this vulnerability will afflict every class and category of networked object. The lesson here is that the security crisis of the internet of things was effectively inevitable, implicit in the ideology of ease and the fundamental proposition of billions of cheap devices installed and managed by ordinary people.

If we are to make our way in a world populated with them, we need to learn how to see these connected things as sites of interest—and particularly as places where our own interests come into contention with those of multiple other parties, the

moment we connect an object with the network that animates it and gives it force.

Consider that staple of the smart home, the networked camera or webcam, whose capacity for remote oversight is generally invoked to secure the people, places or things within its field of vision. This was clearly the intention of the camera installed in the Davao City stockroom, for example, whose operator presumably wished to monitor worker behavior, prevent inventory shrinkage, gather evidence in the event of a theft, and perhaps remind employees that they were visible at all times. Taken together, these aims constitute the interest of the person who installed the camera. Its manufacturer, however, had an interest in keeping its price low, and that meant that the camera shipped without effective provisions for controlling access to it. This in turn served yet another party's interest: that of an intruder, who could probe the local network through this unsecured point of access, and see if there might not be something connected to it worth corrupting, or mobilizing as part of a botnet. These interests all contend in the camera from the first moment it's plugged in, just as your interests and OpenTable's and Google's and a restaurateur's all contend in the Home interface.

What is being gathered together in a Tide-branded Amazon Dash Button? Crack open the case,²² and you'll find a WiFi module and a microcontroller, a microphone, a memory chip and an LED, along with some other harder-to-identify components, all sandwiched on a printed circuit board. The cost of this bill of materials is such that Amazon almost certainly loses a little money with each unit sold—and that's even before considering that they chose to subsidize its purchase in full with a \$5 rebate on the first order made with it.²³ So the first thing that's folded up in the Dash Button is a business model: Amazon wouldn't sell it at all if they didn't know perfectly well they'll be making a healthy profit on everything you buy, on each of the thousand or so occasions you'll be able to press the button before its welded-in battery succumbs.

But what you will also find coiled up in the Dash Button, if you look carefully enough, is a set of standards and protocols

that enfold the agreements of obscure industry working groups on how wireless networking ought to work, incorporating all the tacit assumptions they've made about what a home looks like, what other networked objects you might have at hand, and how bandwidth might be apportioned between them. In fact everything in this proposition seems contingent on something else, everything cascades and invokes some set of settled conventions still further down the line: at minimum the Dash Button assumes that you have a wireless base station at home, and a phone that can run the Amazon app, and most obviously that you have an Amazon account and a line of credit to feed it.

Other facts about the world unavoidably get wound in, too. The temperature in Amazon's fulfillment center, passing-out hot in the summer months because leaving the doors open to let in a breeze would also admit some possibility of theft. The prevalence of miscarriages and cancers among workers in the plant where the gallium arsenide in the LED was made. The composition of leachate in springs fed by runoff from the landfill where the Dash Button will inevitably come to rest in just a few years' time. Your relationship with and feelings about brands—the degree to which you've let the thought "Tide" supplant that of "detergent" in your ordinary awareness, as well as the degree to which you're willing to give that brand real estate in your house. And all of this invoked every time you press the button, just to ensure you never run out of laundry detergent.

There is one more thing that is hidden in the gathering of forces and potentials represented by this little button, more than simply shabby labor relations and some measure of degradation inflicted on the land. It is something that would likely bother a great many of Amazon's customers more than any such nebulous concerns, if they were ever made fully aware of it: that the products sold in this way are subject to Amazon's dynamic pricing algorithm, and therefore that their prices may fluctuate by as much as 25 percent in either direction, anywhere up to several times each day. Strictly speaking, this means that the Dash Button does something a little different every time it is pushed. Anyone wanting to ascertain precisely what it is that

they are paying for their Tide Smart Pouch Original Scent HE Turbo Clean Liquid Laundry Detergent, Pack of Two 48 oz. Pouches will have to seek out that information on the website proper, and this is of course precisely the interaction the Dash Button is designed to forestall and prevent.

The philosopher Graham Harman reminds us that “we live in a world in which things withdraw from awareness, silently enabling our more explicit deeds.”²⁴ But what he doesn’t mention is that very often some party is counting on that withdrawal because it serves their interests. It is not merely for reasons of philosophical curiosity that it is worth our while to haul these reticent things back into the light of day, and open them up for a more considered inspection.

If this imperative holds at the scale of domestic objects and the smart home, it becomes more urgent still when the same set of techniques and practices is applied to the management of urban experience. At this largest scale, the internet of things appears to us as a body of rhetoric around the performance and behavior of the so-called “smart city.” This is a place where the instrumentation of the urban fabric, and of all the people moving through the city, is driven by the desire to achieve a more efficient use of space, energy and other resources. If the ambition beneath the instrumentation of the body is a nominal self-mastery, and that of the home convenience, the ambition at the heart of the smart city is nothing other than control.

Most of us are by now at least distantly aware that our phones, smart or otherwise, are constantly harvesting information about our whereabouts and activities. But we tend to be relatively ignorant of the degree to which the contemporary streetscape itself has also been enabled to collect information. Just as our bodies and homes have become comprehensively instrumented, so too has the terrain through which we move.

The broadest range of networked information-gathering devices are already deployed in public space, including cameras; load cells and other devices for sensing the presence of pedestrians and vehicles; automated gunshot-detection microphones and

other audio-spectrum surveillance grids; advertisements and vending machines equipped with biometric sensors; and the indoor micropositioning systems known as “beacons,” which transact directly with smartphones.

Perhaps mercifully, the average pedestrian is at best only liminally aware of the presence or operation of these sensors. From the sidewalk, they appear as a retrofitted profusion of little-noticed and more or less inexplicable pods on façades and lampposts, a fractal encrustation built up from devices of wildly varying age, type and provenance. With the exception of CCTV cameras—most of which are very much meant to be seen²⁵—these devices are not of any particularly obvious telltale shape. Some are literally embedded in the walls; others are sealed away beneath the street surface, with nothing more than the occasional shiny seam in the paving or the Day-Glo annotations of utility personnel to betray their presence. Very often, they’re quite literally black boxes, mute little oblongs of polycarbonate lampreyed to a building-front, easy to overlook in the rush of daily life. However opaque they may be, though, and whatever the original inspiration underlying their placement, all of these things are ultimately there for a single purpose: to gather facts about some condition or activity transpiring in the public way, and raise them to the network.

Given the enduring, if not increasing, significance of weather in our lives, it should surprise nobody that many urban sensors are intended to gather meteorological information. These measure ambient temperature, precipitation levels and barometric pressure; wind velocity and direction; and multiple indices of air quality, including ozone level and pollen and particulate count. Increasingly often, such meteorological stations are equipped with sniffers designed to scan for the molecular traces of nuclear, chemical, biological, radiological or high-explosive weapons of mass destruction.

Inevitably, a great deal of such sensor deployments have to do with the daily exigencies of municipal administration, whether these be the detectors that measure the average speed of traffic and the velocity of individual vehicles; the soil moisture and pH

monitors that give maintenance crews insight into the health of street trees and plantings; or the automated gunshot-detection systems that recognize the distinctive acoustic signature of a firearms discharge, and (at least in principle) dispatch public-safety resources to investigate.

Many systems in this category are intended to regulate or manage the behavior of another infrastructure. Water-distribution and sewerage networks are increasingly provisioned with their own dedicated grid of sensing devices, in the hope that emergent anomalies in their behavior or performance can be detected early, and dealt with while they're still of manageable scale. The same can be said for the infrastructural networks we more ordinarily encounter directly: the networked bollards and gates that block the flow of traffic into arterials generally rely on some kind of inductive sensor grid, buried beneath the pavement, to register the presence of vehicles. Similarly, the sensors for detecting that a parking space is available, a shared bicycle has been returned to its rack, or a recycling bin is full and needs to be emptied.

Other systems are emplaced in the street because they help administrators regulate behavior more indirectly. This is the intention behind most of the CCTV systems we encounter in public space, whether municipal or private in ownership; over time, these will tend to be provisioned with advanced capabilities like face-detection and -recognition and gaze tracking.²⁶ Similar things can be said for the automated license-plate readers many police departments now equip their fleets with, surprising nobody with the revelation that they are disproportionately likely to be deployed in poor neighborhoods.²⁷ We can think of these as devices that embody, articulate and concretize the gaze of the state, and of other interested parties, as it is brought to bear on people moving through the public way.

Newer systems aim to discover patterns of fact pertinent to commercialization of the sidewalk frontage, detecting how many people are present at each given hour of the day; what they are paying attention to; and, if possible, what demographic or psychographic categories they belong to. Typical of these

is Placemeter, an “open urban intelligence platform” which promises its users the ability to “see how busy places are in real time.”

An increasing number of sensors find their way to the street thanks to the prerogatives of citizen science, and the desire to gather data that supplements (or for that matter, corrects) the official government line on air quality, decibel levels, or radiation. The best-known example of this is the rooftop air-quality station maintained by the US Embassy in Beijing, whose readings are broadcast worldwide over Twitter, making it one of the few sources of information about pollution available to Chinese citizens beyond reach of interference from their government. This is entirely laudable, as are the sensors that underwrite assistive technologies—for example, the beacons deployed in the hope that they might enable visually impaired people to make their way through the city independently.

Sometimes it’s not quite clear why a sensor is there at all. This may be because some party has arrived at a reasoned judgment that the cost of deployment is likely to be outweighed by the potential future value of the data collected, even if it’s not yet clear what that value is. It may be because the sensor is little more than a gesture in the direction of contemporaneity and hipness. Or it may well be that the instrumentation is all but pointless, betraying a profound misunderstanding of what networked data is or how it might be used.

Often, a party pursuing some higher-order ambition fuses sensors of multiple types into a single functional ensemble. New York City’s Midtown traffic management system,²⁸ for example, integrates data from lamppost-mounted cameras²⁹ and microwave traffic-detection arrays, taxicab GPS units, inductive loops in the roadway, and the EZPass electronic toll collection system.³⁰ This is the case in Copenhagen as well, where the adaptive traffic signals integrate data garnered from sources as varied as mobile phones, bicycle sensors in the roadway, and hardware installed in the light standards themselves.

And finally, not everything drawing data off activity on the street is a sensor *per se*. An example, and an important exception

to the general rule of imperceptibility, is that class of systems designed to be overt precisely because they function primarily as interfaces with a networked service of some sort. The classic example would be an ATM, but we can include parking meters, transit-fare kiosks and even vending machines in this category. The data produced by such devices tends to be incidental to their primary purpose, but it is produced and uploaded to the network nonetheless: who was in this place to use this device, at what time, to achieve what end?

The picture we are left with is that of an urban fabric furiously siphoning up information, every square meter of seemingly banal sidewalk yielding so much data about its uses and its users that nobody quite yet knows what to do with it all. And it is at this scale of activity that the guiding ideology of the whole internet of things enterprise comes into clearest focus.

We see the strongest and most explicit articulation of this ideology in the definition of a smart city offered by the multi-national technology vendor Siemens³¹: “Several decades from now cities will have countless autonomous, intelligently functioning IT systems that will have perfect knowledge of users’ habits and energy consumption, and provide optimum service ... The goal of such a city is to optimally regulate and control resources by means of autonomous IT systems.”³²

There is an implicit theory, a clear philosophical position, even a worldview, behind all of this effort. We might think of it as an unreconstructed logical positivism, which among other things holds that the world is in principle perfectly knowable, its contents enumerable and their relations capable of being meaningfully encoded in the state of a technical system, without bias or distortion. As applied to the affairs of cities, this is effectively an argument that there is one and only one universal and transcendently correct solution to each identified individual or collective human need; that this solution can be arrived at algorithmically, via the operations of a technical system furnished with the proper inputs; and that this solution is something which can be encoded in public policy, again without distortion. (Left unstated, but strongly implicit, is the presumption that whatever

policies are arrived at in this way will be applied transparently, dispassionately and in a manner free from politics.)

Every single aspect of this argument is problematic.

Perhaps most obviously, the claim that anything at all is perfectly knowable is perverse. When Siemens talks about a city's autonomous systems acting on "perfect knowledge" of residents' habits and behaviors, what they are suggesting is that everything those residents ever do—whether in public, or in spaces and settings formerly thought of as private—can be sensed accurately, raised to the network without loss, and submitted to the consideration of some system capable of interpreting it appropriately. And furthermore, that all of these efforts can somehow, by means unspecified, avoid being skewed by the entropy, error and contingency that mark everything else that transpires inside history. The greatest degree of skepticism is advisable here. It's hard to see how Siemens, or anybody else, might avoid the slippage that's bound to occur at every step of this process, even under the most favorable circumstances imaginable.

However thoroughly sensors might be deployed in a city, they'll only ever capture the qualities about the world that are amenable to capture. As the architect and critical-data scholar Laura Kurgan has argued, "we measure the things that are easy to measure ... the things that are cheap to measure,"³³ and this suggests that sensors, however widely deployed, will only ever yield a partial picture of the world. So what if information crucial to the formulation of sound civic policy is somehow absent from their soundings, resides in the space between them, or is derived from the interaction between whatever quality of the world we set out to measure and our corporeal experience of it?

Other distortions may creep into the quantification of urban processes. Actors whose performance is subject to measurement may consciously adapt their behavior to produce metrics favorable to them in one way or another. For example, a police officer under pressure to "make quota" may issue citations for infractions she would ordinarily overlook,³⁴ while conversely, her precinct commander, squeezed by City Hall to present the city

as an ever-safer haven for investment, may downwardly classify a felony assault as a simple misdemeanor. This is the phenomenon known to viewers of *The Wire* as “juking the stats,” and it’s particularly likely to occur when financial or other incentives are contingent on achieving some nominal performance threshold.³⁵ Nor is this manipulation the only factor likely to skew the act of data collection; long, sad experience suggests that the usual array of all-too-human pressures will continue to condition any such effort—consider the recent case in which Seoul Metro operators were charged with using CCTV cameras to surreptitiously ogle women passengers, rather than scan platforms and cars for criminal activity as intended.³⁶

What about those human behaviors, and they are many, that we may for whatever reason wish to hide, dissemble, disguise or otherwise prevent being disclosed to the surveillant systems all around us? “Perfect knowledge,” by definition, implies either that no such attempts at obfuscation will be made, or that any and all such attempts will remain fruitless. Neither one of these circumstances sounds very much like any city I’m familiar with.

And what about the question of interpretation? The Siemens scenario amounts to a bizarre compound assertion that each of our acts has a single salient meaning, which is always and invariably straightforwardly self-evident—in fact, so much so that this meaning can be recognized, made sense of and acted upon remotely by a machinic system, without any possibility of mistaken appraisal. The most prominent advocates of this approach appear to believe that the contingency of data capture is not an issue, nor is any particular act of interpretation involved in making use of whatever data is retrieved from the world in this way.

When discussing their own smart-city venture, senior IBM executives argue,³⁷ in so many words, that “the data is the data”: transcendent, limpid and uncompromised by human frailty. This mystification of “the data” goes unremarked upon and unchallenged in the overwhelming majority of discussions of the smart city. But surely these intelligent and experienced

professionals know better. Different values for air pollution in a given location can be produced by varying the height at which a sensor is mounted by a few meters. Perceptions of risk in a neighborhood can be transformed by slightly altering the taxonomy used to classify reported crimes.³⁸ And anyone who's ever worked in opinion polling knows how sensitive the results are to the precise wording of a survey. The fact is that the data is never "just" the data, and to assert otherwise is to lend inherently political and interested decisions regarding the act of data collection an unwonted gloss of neutrality and dispassionate scientific objectivity.

The bold claim of perfect knowledge appears incompatible with the messy reality of all known information-processing systems, the human individuals and institutions that make use of them and, more broadly, with the world as we experience it. In fact, it's astonishing that any experienced engineer would ever be so unwary as to claim "perfection" on behalf of any computational system, no matter how powerful.

The notion that there is *one and only one solution* to urban problems is also deeply puzzling. With their inherent diversity and complexity, we can usefully think of cities as *tragic*. As individuals and communities, the people who live in them hold to multiple competing and equally valid conceptions of the good, and it's impossible to fully satisfy all of them at the same time. A wavefront of gentrification can open up exciting new opportunities for young homesteaders, small retailers and craft producers, in other words, but tends to displace the very people who'd given a neighborhood its desirable character and identity in the first place. An increased police presence on the streets of a district reassures some residents, but makes others uneasy, and puts yet others at definable risk. Even something as seemingly straightforward and honorable as an anticorruption initiative can undo a fabric of relations that offered the otherwise voiceless at least some access to local power. We should know by now that there are and can be no Pareto-optimal solutions for any system as complex as a city.³⁹

That such a solution, if it even existed, could be *arrived at*

algorithmically is also subject to the starker doubt. Assume, for the sake of argument, that there did exist a master formula capable of resolving all resource allocation conflicts and balancing the needs of all of a city's competing constituencies. It certainly would be convenient if this golden mean could be determined automatically and consistently, via the application of a set procedure—in a word, algorithmically.

In urban planning, the idea that certain kinds of challenges are susceptible to algorithmic resolution has a long pedigree. It's present in the Corbusian doctrine that the ideal and correct ratio of spatial provisioning in a city can be calculated from nothing more than an enumeration of the population, it underpins the complex composite indices Jay Forrester devised in his groundbreaking 1969 *Urban Dynamics*, and it lay at the heart of the RAND Corporation's (eventually disastrous) intervention in the management of 1970s New York City.⁴⁰ No doubt part of the idea's appeal to smart-city advocates, too, is the familial resemblance such an algorithm would bear to the formulae by which commercial real-estate developers calculate air rights, the land area that must be reserved for parking in a community of a given size, and so on.

These are tools developers already know how to use, and in the right context and at the appropriate scale, they are surely helpful. But the wholesale surrender of municipal management to an algorithmic toolset seems to repose an undue amount of trust in the party responsible for authoring the algorithm. At least, if the formulae at the heart of the Siemens scenario turn out to be anything at all like the ones used in the current generation of computational models, critical, life-altering decisions will hinge on the interaction of poorly defined and surprisingly subjective values: a "quality of life" metric, a vague category of "supercreative" occupations, or other idiosyncrasies along these lines.⁴¹ The output generated by such a procedure may turn on half-clever abstractions, in which a complex circumstance resistant to direct measurement is represented by the manipulation of some more easily determined proxy value: average walking speed stands in for the more inchoate "pace" of

urban life, while the number of patent applications constitutes an index of “innovation.”

Quite simply, we need to understand that the authorship of an algorithm intended to guide the distribution of civic resources is itself an inherently political act. And at least as things stand today, nowhere in the extant smart-city literature is there any suggestion that either algorithms or their designers would be subject to the ordinary processes of democratic accountability.

And finally, it’s supremely difficult to believe that any such findings would ever be encoded in public policy, and applied transparently, dispassionately and in a manner free from politics. Even the most cursory review of the relevant history suggests that policy recommendations derived from computational models are only rarely applied to questions as politically sensitive as resource allocation without some intermediate tuning taking place. Inconvenient results may be suppressed, arbitrarily overridden by more heavily weighted decision factors, or simply ignored.

The best-documented example of this tendency remains the work of the New York City-RAND Institute, explicitly chartered to implant in the governance of New York City “the kind of streamlined, modern management that Robert McNamara applied in the Pentagon with such success” during his tenure as secretary of defense (1961–68).⁴² The statistics-driven approach that McNamara’s Whiz Kids had so famously brought to the prosecution of the war in Vietnam, variously thought of as “systems analysis” or “operations research,” was first applied to New York in a series of studies conducted between 1973 and 1975, in which RAND used FDNY incident response-time data to determine the optimal distribution of fire stations.

Methodological flaws undermined the effort from the outset. RAND, for simplicity’s sake, chose to use the time a company arrived at the scene of a fire as the basis of their model, rather than the time at which that company actually began fighting the fire. (Somewhat unbelievably, for anyone with the slightest familiarity with New York City, RAND’s analysts then

compounded their error by refusing to acknowledge traffic as a factor in response time.)⁴³

Again, we see some easily measured value used as a proxy for a reality that is harder to quantify, and again we see the distortion of ostensibly neutral results by the choices made by an algorithm's designers. But the more enduring lesson for proponents of data-driven policy has to do with how the study's results were applied. Despite the mantle of coolly "objective" scientism that systems analysis preferred to wrap itself in, RAND's final recommendations bowed to factionalism within the Fire Department, as well as the departmental leadership's need to placate critical external constituencies; the exercise, in other words, turned out to be nothing if not political.

The consequences of RAND's intervention were catastrophic. Following their recommendations, fire battalions in some of the sections of the city most vulnerable to fire were decommissioned, while the department opened other stations in low-density, low-threat neighborhoods—neighborhoods, we may note, which just happened to be disproportionately wealthy and white. The resulting spatial distribution of fire-fighting assets actually prevented resources from being applied where they were most critically needed. Great swaths of the city's poorest neighborhoods burned to the ground as a direct consequence: most memorably the South Bronx, but immense tracts of Manhattan and Brooklyn as well. Hundreds of thousands of residents were displaced, many permanently, and the unforgettable images that emerged fueled perceptions of the city's nigh-apocalyptic unmanageability that impeded its prospects well into the 1980s. Might a less-biased model, or an application of the extant findings that was less skewed by the needs of political expediency, have produced a more favorable outcome? Like all counterfactual exercises, the answers to such questions are unknowable, forever beyond reach. But the human and economic calamity that actually did transpire is a matter of public record.

Examples like this counsel us to be wary of claims that any

autonomous system will ever be entrusted with the regulation and control of civic resources—just as we ought to be wary of claims that the application of some single master algorithm could result in an Pareto-efficient distribution of resources, or that the complex urban ecology might be sufficiently characterized in data to permit the effective operation of such an algorithm in the first place. As matters now stand, the claim of perfect competence that is implicit in most smart-city rhetoric is incommensurate with everything we know about the way technical systems work.

But it also flies in the face of everything we know about how *cities* work. The architects of the smart city have utterly failed to reckon with the reality of power, and the perennial ability of various elites to suppress policy directions they find uncongenial to—that word again—their interests. At best, the technocratic notion that the analysis of sensor-derived data would ever be permitted to drive resource-allocation decisions and other acts of municipal policy is naive. At its worst, though, it is culpably negligent of the lessons of history.

That the available evidence strongly suggests that most such data is never leveraged in this way—that, in fact, the formation of municipal policy is guided by just about any concern other than what the data determines—is immaterial. There will always be an enterprise willing to make these arguments, and in this historical period, anyway, there will always be municipal administrations desperate enough for some insight that they’re willing to sign on the dotted line. There seems to be little that any of us can do to prevent this. But the rest of us are best advised to approach all claims about the smart city and its ostensible benefits with the greatest caution.

At present, the internet of things is the most tangible material manifestation of a desire to measure and control the world around us. But as an apparatus of capture, it is merely means to an end. The end remains the quantification of the processes of life at every scale; their transformation into digital data; and the use of that data for analysis, the development of projective

simulation and the training of machine-learning algorithms. It behooves us to spend some time thinking about what comes along for the ride, every time we invoke this complex of ideas, to consider where it might have come from and what kind of world it is suggesting we live in.

For me, many years of thinking and working in this domain have left behind a clear and vivid picture of that world. It seems strange to assert that anything as broad as a class of technologies might have a dominant emotional tenor, but the internet of things does. That tenor is *sadness*. When we pause to listen for it, the overriding emotion of the internet of things is a melancholy that rolls off of it in waves and sheets. The entire pretext on which it depends is a milieu of continuously shattered attention, of overloaded awareness, and of gaps between people just barely annealed with sensors, APIs and scripts.

Implicit in its propositions is a vision of inner states and home lives alike savaged by bullshit jobs, overcranked schedules and long commutes, of intimacy stifled by exhaustion and the incapacity or unwillingness to be emotionally present. The internet of things in all of its manifestations so often seems like an attempt to paper over the voids between us, or slap a quick technical patch on all the places where capital has left us unable to care for one another.

But for all the reservations we may have along these lines, however sincerely held, they still don't speak to the most sobering circumstance we are confronted with by this class of technologies. This concerns who it is that winds up in possession of the data we shed onto the internet of things, and what they choose to do with it.

Here, heartbreakingly, history furnishes us with a directly relevant case study. In 1936, it became mandatory for each Dutch municipality to maintain a demographic record of its inhabitants; by 1939, each citizen had to carry a *persoonskaart*, or personal identity card. Both included a field for "heritage," or ethnic origin, and this finding was entered alongside all the other facts by which the state Bureau of Statistics characterized its population. This registry was maintained on punched Hollerith

cards, the most advanced data-storage and -processing system available at the time.⁴⁴

We may believe that the collection of such facts is fundamentally innocuous, if not an essential aspect of modern statecraft. We may further repose a significant degree of trust in the institutions responsible, and rest easy in the thought that they have our best interests in mind. Perhaps you feel sufficiently assured of the good intentions of our own duly-elected democratic government, and of the checks on its exercise of power imposed by the rule of law, that the mere existence of tools infinitely more powerful than a Hollerith card reader does not trouble you.

But history is replete with reasons for doubt on all of these counts. Regimes, after all, do change, and closely held state secrets are spilled into the open air. Businesses fail, or are acquired, and whatever property belonged to them passes from their control. “Eternal vigilance” sounds stirring enough, but turns out to be rather hard to maintain over time. So what happens when datasets harvested by institutions we trust pass into other, less benevolent hands—as history suggests they demonstrably and reliably do, whether through systems intrusion, corporate acquisition, or simple human clumsiness?

The Dutch experience is instructive. Both the Hollerith cards on which the civil registry of 1936 was tabulated, and the machines necessary to sort and read them, immediately fell under German control after the invasion of 1940. The same data that was innocuous when provided to the Bureau of Statistics turned out to be lethal in the hands of the Gestapo.

Information that under a liberal administration would have been perfectly harmless was literally weaponized by the Germans and their Dutch collaborators, permitting comprehensive roundups and targeted, efficient door-to-door searches for named individuals. In June 1942, mass deportations began. Approximately 107,000 Dutch Jews were sent to the Mauthausen and Bergen-Belsen concentration camps and the death camps of Sobibor and Auschwitz beyond, the latter places where organized murder took place at industrial scale.⁴⁵ Fewer than five percent of the deportees survived to the end of the Second World War.

What this precedent reminds us is that data can be acted upon to shape the world, leveraged to produce such an outcome. But also: that in some way *this outcome was always already nestled within the data*, from the moment of its collection. This is the grim reality underneath the pat Foucauldian formulation “power/knowledge,” and it stands in sharp rebuke to an age in which we not merely submit to the continuous siphoning of information from our cities, spaces and bodies, but do so willingly and even enthusiastically. As for the commonplace assertion that those who have nothing to hide have nothing to fear, consider the sentiment often attributed to Richelieu, and salient whatever its actual provenance: “If you give me six lines written by the hand of the most honest of men, I will find something in them with which to hang him.” This has never been truer than it is in our age of metadata, when analysis of large bodies of data may turn up correlations we weren’t ourselves aware of, when drone strikes and acts of extraordinary rendition have been authorized for the most glancing and seemingly coincidental constellations of fact.

So, yes: the internet of things is a sprawling and complex domain of possibility, and it would be foolish to avoid investigating it energetically and in good faith. But we would be wise to approach that investigation with an unusually strong leavening of skepticism, and in particular to resist its attempts to gather data regarding ourselves, our whereabouts, our activities and our affiliations, whatever the blandishments of ease, convenience or self-mastery on offer. The Serbian human rights activist Jasmina Tešanović recently described the internet of things as the “project of a technical elite that aspires to universality,”⁴⁶ and in truth that description could apply with as much justice to every technology discussed in this book. Wherever a project has such overtly imperial designs on the everyday as this one, though, it’s imperative for us to ask just what vision of universality is being evoked in it—what vision, and whose.