# The Routledge Companion to Media Studies and Digital Humanities

Author(s) Sayers, Jentery

Imprint Routledge, 2018

ISBN 9781138844308, 9781315730479

Permalink https://books.scholarsportal.info/uri/ebooks/ebooks5/taylorandfrancis5/2019-11-27/4/9781315730479

Pages 222 to 229

Downloaded from Scholars Portal Books on 2023-11-12
Téléchargé de Scholars Portal Books sur 2023-11-12

# 21

# SMART THINGS, SMART SUBJECTS

## How the "Internet of Things" Enacts Pervasive Media

*Beth Coleman*

### Always Crashing in the Same Car

When Charlie Miller and Chris Valasek hacked a Jeep Cherokee in 2015, it was the first known remote-control takeover of an automobile (Greenberg 2015). The coders wrote a patch that got them into the Jeep's control system via a vulnerability in the car's networked entertainment components. During a test drive, the driver gradually lost control. First, the air conditioning system started to blast, and then the radio began blaring. Even though he consented to the test drive, the driver was quickly startled—and then panicked—when Miller and Valasek cut the acceleration while the car was moving down the highway, bringing it to a sickeningly slow pace with cars and trucks amassed behind it. To gain control of the acceleration again, the driver had to pull off the highway and *restart* the vehicle.
The stunt demonstrated several traits of the Internet of Things (IoT):

- networked automation can trump local, autonomous control
- networked technologies have direct impact on our sense of privacy and control
- networked media allows for a hyper-extension of reach and vulnerability.

Known variously as "smart" technologies, ambient intelligence, and social machines, an IoT further extends our reach across networked information (internet and mobile computing) into the material world. There are objects such as "smart" cars that drive themselves and "smart" tiles that tell us where our dumb objects, such as keys and bikes, are hiding. They sense the environment, removing the need for our attention to complete certain tasks (e.g., opening a door or noticing when a traffic light turns green). Among other things, an IoT further automates our physical habitat and daily habits of memory and action. We find ourselves extended, again, with a new level of reach—a remote control that looks a bit like magic—*even as we are rendered more exposed*. Remote control means we can reach and be reached. As demonstrated by the Jeep hack, the extension goes in both directions: more power to act and more vulnerability to be acted upon.

This is a world in which interaction takes pride of place. In fact, such interaction increasingly establishes what "place" means and how we come to inhabit it—what we might call modes of *X-reality*, the merging of informational and physical world (Coleman 2011). Each mode, with its corresponding information and communications technology (ICT), moves the point of transmission increasingly away from a stationary computer and toward mobility, location, and the phenomenal world. But, as the technology gets "smarter," is the human subject getting dumber? Put differently, what does a "smart subject" look like in this configuration?

As illustrated by the car hack, an IoT interaction is fairly *invisible*. It is an interaction based on the conditions of pervasive media in which devices talk to each other, automatically updating agendas, programs, scripts, and so on—creating a network of machine-to-machine (M2M) communication. This M2M communication is so important that the European Technology Platform on Smart Systems defines an IoT as "a world-wide network of uniquely addressable interconnected objects, based on standard communication protocols" (EPoSS 2008). They describe a merger of the informational and material world in which common objects—beyond one's cellphone and tablet—are imbued with computational power that allows them to be identified, activated, or controlled across a network. This is the radio frequency identification (RFID) tag that makes physical packages easy to scan and locate for speedy delivery. These are the data chips in mass transportation cards that say how many people boarded at which station and when they exited. These are "smart" technologies different than other, older computational technologies along two primary lines: they sense information about the physical environment, and they broadcast that information. Industrial age machines, such as thermostats, gauge the temperature and other aspects of their environment. Items such as smart phones and tablets receive and broadcast information. An IoT object such as the Nest "smart" thermostat heats up your house via remote control and transmits temperature data over the course of time (through the month, year, and so on). The device offers a pleasing, streamlined design from physical object to interaction. It also creates a real-time "data portrait" of the heat signature of a household. The question about such pleasing IoT devices is not whether they work (they do), but to whom the information is broadcast.

## Oh! You Pretty Things

One finds important differences between early automation, such as the autopilot program, and pervasive automation, as described by the IoT. These differences are articulated along the lines of technological design, public policy, and the people who use them—"end-users" or citizens, depending on how one describes the relationship. This "depending" gives a false sense of chance operation, a roll of the dice, when in actuality the description of designed objects is also the description of an ontology—the perspective of its framework and properties, as defined by the domain in which it exists—where the affordances (technological aspects) and the social aspects (behaviors around connectivity, privacy, and searchability) are programmed along the lines of specific expectations regarding transparency, service, and ownership.

In this light, what is the difference between the self-driving car of the near future and a plane's autopilot program, a real-time feedback system first introduced in the 1920s? Both automate a procedure that had previously commanded human attention; both "sense" the environment for critical feedback that determines course of action. The "smart" technology, though, is new in its increasing scale of application . . . in its emerging ubiquity. We have

ever more tiny computational devices that can be activated toward interaction with humans and automation with other machines. But the difference does not rest singularly with ubiquitous computing as a technological platform. It also reflects a cultural assumption of *pervasive mediation*—a radical increase in the power of automation. The system design of the autopilot was conceived as prosthesis: when the pilot tired, the autopilot could be engaged for nonemergency conditions. The shift with the driverless car is semantic (how we program its purpose) and procedural (how it enacts its designed functions). The car's smart system becomes the de facto driver—all the time, for all conditions.

"Smart" does not necessitate sentience. But it does involve programming qualities of the sensitive and sensible. Literally, a self-driving car needs to understand the sensory factors of road conditions as well as the sensibility (mood, orientation, etc.) of other drivers on the road. The sensory and affective spectrum must be translated into machine-readable language with a bouquet of real-time, real-world variables. Thus, sensing the environment and acting upon that input is increasingly in the "hands" of machines we have designed. And out of ours.

This is not necessarily bad news for activities such as driving, flying planes, or running the HVAC and lights system. Human judgment is demonstrably not as good at these activities as well-programmed machines (with the exception of some circumstances, such as emergencies). In the narrow view of highway safety, the automation technology keeps getting better, and we are not very good drivers en masse. In the larger scope of a pervasive automation, the outlook is not as sanguine.

In a comprehensive analysis, Anzelmo et al. discuss the formulation of an IoT and the technological, commercial, legal, and social aspects of its development (2011: 6–7). In defining the scope of an IoT, they write, "it is a network of connected objects. *Vehicles, machine components, domestic consumable durables, the clothes on your back*, all are being hooked up to a network with a speed most of us have yet to comprehend" (2, emphasis added). And in fact, what they describe is more or less a technologization of everything. In the history of interaction design and computation, Mark Weiser (chief scientist at Xerox Palo Alto Research Center), first articulated this vision of ubiquitous computing in 1991 when he looked at desktop computing and predicted that the future would be tiny computers and giant touchscreens scattered throughout the environment (Weiser 1991); there would be clouds of computing—ethereal and communitarian—as opposed to static hunks of plastic with awkward interfaces. That is the path we are on with IT companies, such as Apple and Google, leading the way on minimal, pervasive, customized, and closed design.

Although it looks like technology is the issue, in fact it is the social that is at stake. As Anzelmo et al. point out, the implications for this emergent technology reach across domains of technical standards, privacy protection, and politics: "[t]herefore, while many technical challenges remain to be overcome, the main themes and discourse around the Internet of Things are primarily social in scope and intent" (2011: 3). It was only in 2012 that Apple officially released an unlocked iPhone, its series of smart phones, allowing the user to put in a SIM card of her choosing (AT&T). Until that point, the design default had been to lock-up user access to the network information of the device. Despite the fact the one pays a tidy sum to buy the phone, one has to know to ask (and pay) for an unlocked phone or know how to hack it.

The iPhone design delivers sleek form and services with increasing obfuscation of the system of selection, reporting, and delivery. (Is the open OS Android significantly better? Yes and no.) It is certainly a pretty thing that we want, as demonstrated by Apple sales (Williams-Grut 2015). In contrast, one must bring intelligence to the device to know how to handle

its privacy settings that lockout the user. And this is the scenario played out with increasing frequency: *"smart" outlines a particular model of service delivery and data acquisition*. The necessary intelligence to interpret how the device does what it does remains fairly esoteric.

A key aspect of the hard-to-know smart systems of algorithmic recommendations and cloud computing (where "our" bits are and how they are being served up) is that *they are not for us*. The data are not part of the user experience of "smart." The data are for the machines to learn faster in a M2M capacity. Such a machinic dialogue can be found in the quotidian act of your cellphone talking to wifi networks it "knows" (or has accessed in the past) without having to ask you. In the right hands, your bicycle and your washing machine reveal forensic evidence. We have programmed our cellphones and thermostats and cars to remember for us, to find our way, to make us feel at home. In this role of helpmate, the machines tell on us, describing our everyday in a newly intimate manner. Our acts are legible as data, if someone cares to read this affective broadcast.

## We Pack and Deliver Like UPS Trucks

The Tile IoT technology is a small, white plastic disk no bigger than a quarter, if a quarter were square. The Tile works as a tracking device, signaling its location to one's phone using a micro Bluetooth tracker—for home (short range) and outside (distance) use. In either case, it is a device-to-device communication with the human as the end-user in the exchange of information. In the case of short-range wireless connection, within 100 feet the Tile can transmit its location and that of the item to which it is attached—keys, wallet, dog collar, and so on—to the phone running the Tile app. The Tile signals its location with a loud tone until it is located. At greater distances, the Tile will use *other* people's phones to signal location, a kind of M2M relay, until the location is broadcast to the Tile owner. Notably, for distance broadcast, the cellphones that form the informational chain run the app *outside the supervision of their humans*, who must enable background "community" support, after which the tracking is anonymous.

Short-range Tile use is fairly quotidian (which does not make it *secure*). We have long been able to program our IT machines with tracking devices so we can find them in local range (e.g., "Find My iPhone" became a standard application when the iPhone 1 entered the 2007 market at $500). The question of what information telecom and internet providers possess about users remains primarily a background one because these companies have had access to this information since the beginning of mobile telephony. The fact that noncomputational objects, such as keys, can now signal location is the reason Tile exists as a commercial endeavor. Yet the most significant change relates to a shift in register in M2M engagement. The civic, or perhaps one must say "public," use of the app presents a new form of IoT interaction that invokes the idea of a "community" of users who enable their devices to help crowd-solve the problem of a stolen bike or missing purse. This next level of machinic communication allows devices from an ad hoc Bluetooth network to ambiently track an object across a territory. Thus, a secondary effect of the Tile device finding your things for you is a *mapping* of things: where things go and how they can be found becomes an aggregated heap of data of how Tile *users* (you) move around the city. (And this is a distinctly urban app; it requires locative density of users to function as a "community.")

As with the transit smart cards introduced in Hong Kong, London, and Amsterdam, the issue of efficiency (getting on the train without stopping to buy a ticket) provides a great deal of data on how people use public transportation. This data can help with issues of traffic flow, congestion, and so on. It makes sense to have civic data on how the trains run.

But to have civic data on how *people move* requires a degree of transparency and protection of privacy that does not yet exist. The Tile tracking device, without stating it, invites one to opt into a level of precision tracking at an unprecedented scale. The closest corollary to this locative technology is an ankle monitor, the mandatory IoT bauble of those under house arrest so authorities can remotely monitor their location. (The ankle monitor uses radio frequency and global positioning systems for local and distance broadcast.) Or, we could imagine ourselves as packages en route for delivery with an available status update at any point along the way, much like delivery services such as UPS and FedEx keep track of their shipments once the objects leave the dispatch point. Historically, governments and businesses had to go through a lot of trouble to track the movements and activities of their citizens. Because our environment reaches increasingly toward a full broadcast of all actions that can be translated into digital information (e.g., purchases, "likes," steps, heartbeats, and location), the only way not to participate in a Big Data surveillance society is to take great pains to opt out.

The curtailing of civil rights is neither abstract nor far off. The Tile promotional video describes a scene where a young woman's bike is stolen. The network of connected devices (smart phones running the Tile app in the background) send an alert, tracking the object through the streets of the city, then anonymously relaying its position to the owner. If one plays out the implied Tile scenario, then one sees the community of good users—the good looking, global creative class made up of people who live in renovated industrial spaces and exercise a lot. We do not see the perpetrator of the crime: the bike thief. One can only imagine that the perp is *someone else*—someone not imagined in the neoliberal system of things and services.

As a tracking device, the Tile accelerates locating the purloined object and, one must assume, the person who took it . . . or the person in whose hand it is found. It further automates a ruthless social logic of have and have not where we can track people who take our stuff *without* ostentatious surveillance equipment or law enforcement. The Tile does not make someone steal a bike, but it does accelerate an automation of crime and punishment that further truncates presumption of innocence and contextual nuance. It closes down on a logic of inclusion and exclusion that only reinforces societal expectations of who makes up a criminal underclass of petty crime. And yet, this is only the cover story of services delivered. In its promise of efficiency, the Tile also tracks "us."

The orientation of IoT design is not a democratic process; the development is accelerated by the global network economies manifested with the second wave—the world wide web and e-commerce—of the internet. The biggest media companies in the world dominate it: Apple, General Electric, Google, Microsoft, Amazon, Siemens, and Facebook, with huge activity around Smart City builds from IBM, Intel, AT&T, and Cisco, among others. The IT industry loves Smart Things, and that love is the primary reason a new robot uprising (small AI, not big AI) is taking place. Smart objects signal a massive expansion of computational objects. Peter Semmelhack, founder of the open-source hardware company Buglabs, explains that the business future of "social machines" cannot be underestimated: "Right now there is an enormous pool of untapped information residing in all of the machines we've designed, built, and launched into the world" (2013: 28). However, Semmelhack makes clear in his IoT business model that this future does not *preclude* design that makes data both transparent and open. In other words, there are possibilities for design protocols that grant us control over when we want to be located and when we do not.

People have found their own workarounds for the always-on, always-identifiable dimensions of ubiquitous computing. Turning off networked devices, purchasing "burner" phones, encrypting information, redirecting IP addresses, anonymous darknets . . . these are

all strategies from the hacker underworld that have emerged in everyday practices of regular people. Certainly, the IoT is not a design culture without its distributed disruptions—its pockets of citizen makers and hackers who innovate toward degrees of freedom. "Faraday pockets" that sheath cellphones from remote snooping emerged as the cool accoutrement of the digerati in 2015 (Lomas 2014). This IoT pocket protector is a charming object within a high-tech consumer culture where "we" are in control ("we" being educated and privileged ICT users, who are often the same class as ICT makers). Needless to say, the Faraday pocket does not address the systemic issues of ubiquitous data collection.

Such affordances to protect or alert are not common practice in IoT design because there is interest neither in the tech community nor among users to make available the valuable data gleaned from IoT devices. Transparency is far outside of our cultural habits around ICTs. Activists and outlaws have plenty of practice with these issues, but normal citizens do not. Bruce Sterling makes this point when he states:

> The real problem . . . is that the reader thinks he's the hero of the story. To the vacuum company, he was the "customer" or "consumer." In the legacy internet days, he was the "user." In the Internet of Things, he lacks those privileged positions, "user" and "customer." An Internet of Things is not a consumer society. It's a materialised network society. It's like a Google or Facebook writ large on the landscape.
>
> (Sterling 2014: 26–29)

He identifies a shift in subject position outside the inherited consumer model that has arisen quickly as a societal norm (i.e., "free" services for user information). Additionally, in materializing the informational network, the IoT forecasts a world of ubiquitous computing where everything is animated around us (Coleman 2012).

One effect of augmenting everyday objects and the built environment is a new norm of seemingly unfettered access, which is mostly a smokescreen. If we look at the situation in relation to interaction and ubiquitous computing, this model breaks down very quickly across several dangerous avenues. The two most egregious are privilege (for whom are these services designed) and exclusion from system knowledge (who has access to this information). What Guy Debord theorized as the seductive "spectacle" of the twentieth century and Baudrillard as the procession of "simulacra," the IoT takes a turn of the screw *beyond*, toward a material interaction that inhabits the landscape. And we find ourselves "participating" in that system of information collection: surrounded by sensor networks and surveillance cameras while carrying tracking devices.

Around the cultural edges of this massive technological build, we are beginning to hear voices calling for the Smart Subject to become a Smart Citizen—activated and engaged in a battle for (degrees) of autonomy—who is the civic face of ubiquitous technology systems. Against the IoT endgame, author and open internet advocate, Cory Doctorow, analyzes the progression of a surveillance society through a historical lens: first, it is the criminals who are stripped of rights, then the infirmed and children on whom tactics of control and surveillance are auditioned. After, these techniques are applied to society as a whole (Doctorow 2015). By waiving our rights for services ("free"), we participate in this development whether we know it or not.

What the IoT design ontology still lacks are the civic aspects of free and open—and not simply as developer tools. Increasingly, civic media design is a growing demand. Groups such as Future Everything have corralled advocacy for this position across diverse sectors

of academic, technological, and activist work. This ad hoc group takes the position that a Smart Citizen paradigm must include Smart Things with trackable, transparent activity. It is in fact citizens who need to take the lead in programming our "smart" future:

> On the one hand there is the view that Smart City design should allow for the disruptive ways in which people use technology. But there is also a stronger claim here, namely that citizens can, and should, play a leading role in conceiving, designing, building, maintaining our cities of the future.
>
> (Hemment & Townsend 2015: 2)

In how Future Everything names the problem and points toward a solution, one can only be struck by the incredible difficulty of "seizing" the means of the production. This really would be a revolution.

## Call Me Maybe

So who is the driver in the world of the driverless car? The steersman of cybernetics is not the human driver but the system (Weiner 1965). However, important aspects of that system are *programmed* toward particular outcomes. We can data mine to optimize website use and make recommendations (common uses of Big Data). Or we can data mine to solve traffic problems (another common use of Big Data). We might also data mine phenomena such as the distribution of wealth and educational resources (e.g., Occupy Wall Street), environmental monitoring (Amsterdam Smart Citizen Lab), and so on. These are issues that civic activist groups rally around, and they call for more open access to databases as well as a transparent formulation of what data has been acquired and under what conditions. As critics of the coming IoT have noted, there is more complexity in the *social adoption and ethical standards* than in the technical development of this next turn in networked media design.

The terror (and the glory) of the IoT is not the singularity—the robotic "last days" that movies such as the *Terminator* series and a long line of sentient AI speculative fiction describe. Rather, the terror is losing all standards of decorum—of a right to self and unfettered relation to others. Decorum is a Latinate word meaning, "right and proper," which in modern parlance essentially means, "good manners." In calling for the rights and property of the Smart Subject, I suggest the root meaning. And in advance of "smart" systems, advocates of the Smart Citizen ask for a mandate of decorousness—a kind of decency in the design and use of IoT technologies.

This is a change away from the raging consumer service model; such an economy simply fulfills the user pleasure principle and only accelerates the role of humans as one Smart Thing among others. Change would thus entail new design ontologies based more closely on open-source and open-civic platform models, and it would prescribe a societal awareness of how (and why) these technologies work. Which is to say, the massive adoption of a Smart Citizen view is highly unlikely. It cannot simply be legislated, even if there were the political will. To ask people to *desire* decorum around privacy, ownership of one's data, and knowledge of public data systems is a tall order.

What, then, is the territory between abandoning control and developing better systems for sustainability? Can we have our benign IoT and eat it too? Probably not. But maybe. It depends on how collective awareness of these technologies develops and what fuels it. Based on the mass adoption of social media in the early 2000s, prospects are not great. Yet, as noted, one finds growing communities of discontent and refusal that take diverse

manifestations. As the avatar Citizen Four, Edward Snowden's self-immolation in the world of national security certainly served as a catalyst for awareness.

There is no IoT outside of a surveillance network. The hacks, the points of resistance, the increased awareness of how such information systems behave are the best options if one is to imagine a *free agent* within the context of pervasive mediation and ubiquitous computing. If machines are now part of a sensing system, increasingly interpreting sense and sensibility, then the differential rests with an ability to be a good actor—that is, decorous *and* contentious, working toward comprehension. "Smart" is shorthand for outsourcing information and responsibility. If intelligence implies *an act of interpretation*, then we have an opportunity at this turning point to discern between convenience (what looks like more free services) and engagement (what looks like more hard work). Otherwise, we will indeed always be crashing in the same car.

## References


Anzelmo, E., A. Bassi, D. Caprio, S. Dodson, R. van Kranenburg, and M. Ratto. (2011) "Discussion Paper on the Internet of Things," Berlin, Germany: Alexander von Humboldt Institute for Internet and Society.

AT&T (n.d.) "Unlock Phone or Tablet," retrieved from www.att.com/esupport/article.html#!/wireless/KM1008728.

Coleman, B. (2011) *Hello Avatar: Rise of the Networked Generation*, Cambridge, MA: MIT Press.

Coleman, B. (2012) "Everything Is Animated," Special Issue on "Animation and Automation," *Body & Society* 18(1), 79–98.

Doctorow, C. (2015) "Art, Design, and the Future of Privacy," Panel held at *Pioneer Works*, September 17, retrieved from boingboing.net/2015/09/09/nyc-to-do-art-design-and.html.

EPoSS (2008) "Beyond RFID—The Internet of Things," retrieved from www.smart-systems-integration.org/public.

Greenberg, A. (2015) "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, retrieved from www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

Haraway, D. (1988) "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective," *Feminist Studies* 14(3), 575–99.

Hemment, D. and A. Townsend (2015) "Here Come the Smart Citizens," in D. Hemment and A. Townsend (eds.) *Smart Citizens*. Manchester, UK: Future Everything Publications, pp. 1–3.

Lomas, N. (2014) "UK Menswear Brand, The Affair, Wants to Make Privacy Tech a Fashion Statement," *TechCrunch*, retrieved from techcrunch.com/2014/09/04/unpocket.

Semmelhack, P. (2013) *Social Machines: How to Develop Connected Products that Change Customers' Lives*, New York, NY: Wiley.

Sterling, B. (2014) *The Epic Struggle of the Internet of Things*, Kindle Edition, Moscow, Russia: Strelka Press.

Weiner, N. (1965) *Cybernetics: Or Control and Communication in the Animal and the Machine*, 2nd edn, Cambridge, MA: MIT Press.

Weiser, M. (1991) "The Computer for the 21st Century," *Scientific American* September, 94–104.

Williams-Grut, O. (2015) "Apple's iPhone: The Most Profitable Product in History," *Independent*, retrieved from www.independent.co.uk/news/business.

Wolfe, C. (2009) *What Is Posthumanism?* Minneapolis, MN: University of Minnesota Press.