Rob Kitchin | Continuous Geosurveillance in the “Smart City”

Keywords: big data, computing, control creep, data issue, geosurveillance, ICT infrastructure, mark dorf, monitoring, original artwork, predictive profiling, Rob Kitchin, sensors, smart city, social sorting, Software, surveillance, tracking, ubiquitous computing, urban landscapes

New forms of governance in the era of ubiquitous computing

Continuous Geosurveillance in the “Smart City”

Rob Kitchin on the New Forms of Governance in the Era of Ubiquitous Computing

With original artwork by Mark Dorf

Mark Dorf, Nebulous 03, 2015

For the past couple of decades there has been a steady stream of analysis that has documented the ways in which the rollout of new digital and networked technologies have enabled increasingly pervasive and extensive forms of state and corporate surveillance. Such technologies have the capability to capture and communicate data about their use; simultaneously a wealth of sophisticated software has been developed that processes and acts on such data in automated, autonomous, and automatic ways. Importantly, the use of embedded GPS, sensors, and digital cameras are enabling location and movement to be tracked, facilitating extensive geosurveillance of people and places.

Continuous geosurveillance relies on the production of spatial big data, and in particular the notion of the “smart city” takes center stage, that is, urban landscapes that can be monitored, managed and regulated in real-time using ICT infrastructure and ubiquitous computing. Such instrumented cities are promoted as providing enhanced and more efficient and effective city services, ensuring safety and security, and providing resilience to economic and environmental shocks, but they also seriously infringe upon citizen’s privacy and are being used to profile and socially sort people, enact forms of anticipatory governance, and enable control creep, that is re-appropriation for uses beyond their initial design.

What follows is a consideration of the unfettered rush to create “smart cities” that is sensitive to the risks involved in extensively monitored urban landscapes. Are too much data about people and places being generated by public and private institutions and used to profile, sort, and sift in pernicious ways? In the rush to create smart cities is the privacy and freedom we expect in liberal democracies being eroded? Perhaps most alarming, are we creating cities that represent the interests of a select group of corporations and technocrats, rather than producing ones that represent the best interests of all citizens?

Extensive and Continuous Geosurveillance

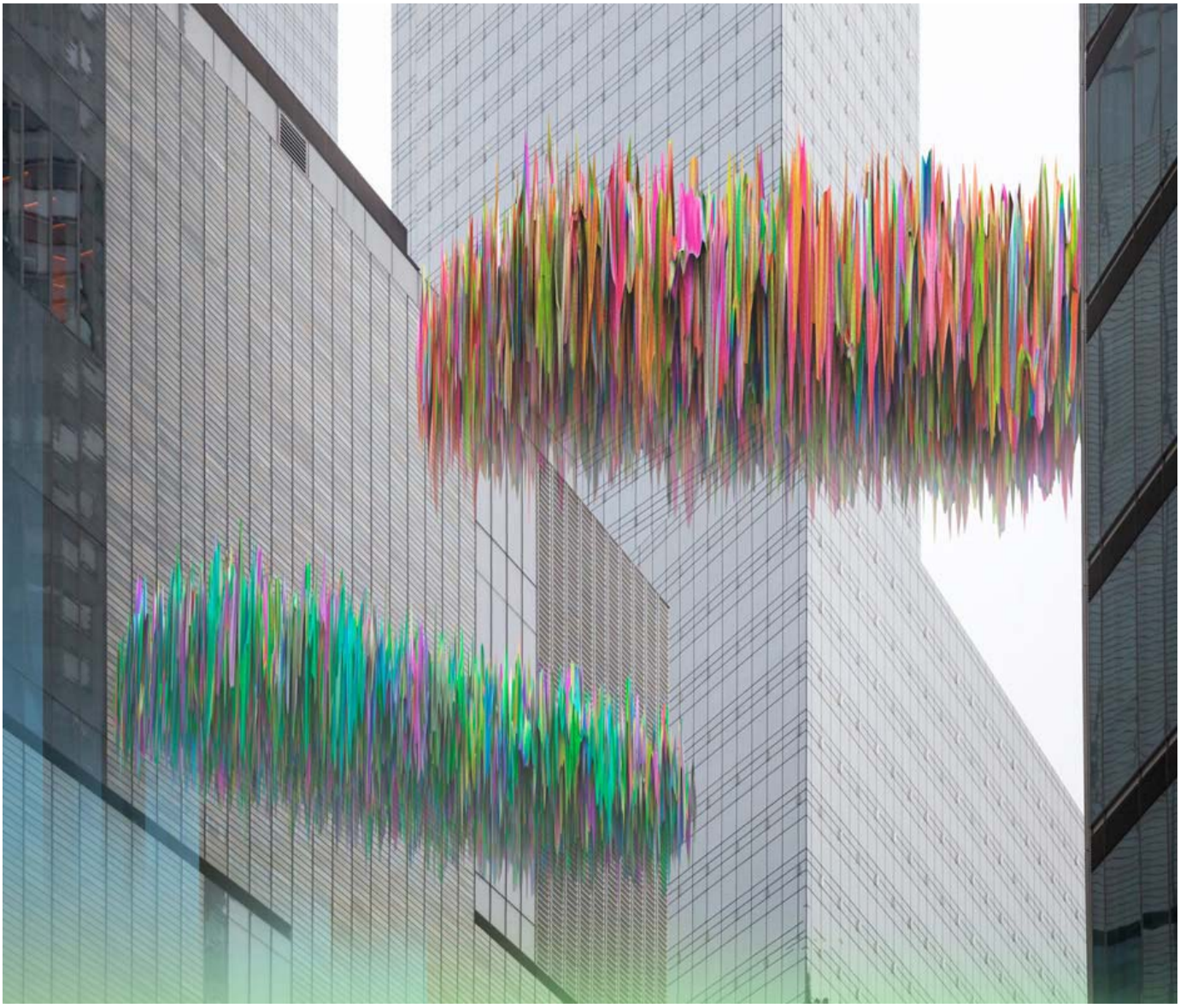
If we wind the clock back seventy years, surveillance was generally a slow, labor-intensive, and partial process. Two of the largest cutting edge surveillance operations of the Second World War — the Bletchley Park decryption of encoded messages and the Medmenham air photo reconnaissance — sought to determine the location and likely movements of troops and equipment across Europe and the Atlantic ocean. Both required thousands of well-trained personnel to work through massive amounts of sampled analogue material of variable quality to map the enemy. The records were bulky, difficult to cross-tabulate and analyze, and expensive to store. Interpretation was imprecise and often quite granular. The only way to track the movements of an individual, and their patterns and preferences of consumption, were to follow them in person and to quiz those with whom they interacted. As a result, nearly everybody passed unobserved in the crowd unless there was a specific reason to focus on them through the deployment of costly resources.

Today the situation has changed utterly. An abundance of networked digital devices, systems and infrastructures mediate movement, work, consumption, communication, and play. We are at the beginning of an era of ubiquitous computing, enabled by advances in computation, data analytics and machine learning, internetworking, and database solutions that facilitate the harvesting, processing, analysis, storage and sharing of vast quantities of data, often in real-time and at a fine resolution. Consequently, citizens and spaces have become knowable and governable in new ways.

Satellites and drones can monitor large portions of the planet at highly granular resolutions, taking up fixed orbits to provide a continuous stream of data about a location. For example, the ARGUS-IS project, unveiled by DARPA and the US Army in 2013, is a 1.8-gigapixel video surveillance platform operated from a drone with a resolution of six inches from an altitude of 20,000 feet. Capturing 12 frames per second the system can track in real-time up to 65 moving objects (Anthony 2013). Many cities are saturated with remote controllable digital CCTV cameras that can zoom, move and track individuals and objects such as vehicles, with analysis and interpretation aided by algorithmic analyses, such as facial, gait and automatic number plate recognition. In cities such as London and New York it is all but impossible to traverse the city unnoticed, with trains, stations, buses and pedestrians nearly

always in sight of a digital CCTV camera, and large parts of the road network surveyed by traffic, red-light, congestion and security cameras.

Cameras are increasingly being complemented with interconnected sensors and actuators embedded into the fabric of cities that form one element of the Internet of Things. These can measure specific outputs such as levels of light, humidity, temperature, chemicals, electrical resistivity, acoustics, air pressure, movement, speed, water levels and quality, and so on, creating a continuous stream of data. Placed on vehicles, they can monitor location, workload, stress, and terrain. By attaching RFID chips to products it becomes possible to track and trace the movement of individual units from factory or farm to consumer. Likewise, RFID tags in vehicles communicate with transponders at toll-booth and parking barriers, enabling automatic payment, as well as measuring vehicle flow or parking space availability. Similar units attached to buses and trains communicate with transponder boxes along their routes making it possible to track the location of vehicles in real-time.



Mark Dorf, Nebulous 07, 2015

Machine-readable ‘smart cards’, such as the London’s Oyster Card, scanned when entering and exiting stations or buses means that it is possible to trace individual journeys across the bus and rail system for two million passengers a day. Cards to enter and progress through buildings enable localised logs of movement. Moreover, sensor boxes are now being

deployed on garbage bins or lampposts that scan passing mobile phones for their unique identifiers, tracking the movement of pedestrians from one box field to another. The PlanIT Valley development in Portugal, presently under-construction and designed for up to 225,000 inhabitants, aims to create a built environment laced with over 100 million embedded sensors that will produce data to monitor a diverse range of infrastructures and environments (see Marchetti 2012).

Through the embedding of chips and software into their design objects have now been made ‘smart’, able to generate, process and react to data inputs, and to communicate these data to third parties. Even the most quotidian devices are full of powerful software, as well as gyroscopes, accelerometers, compasses and GPS, that sense movement and location. Location-based social networking (LSBN) apps such as Foursquare and location-based service apps, such as Hailo and Uber, and mapping/routing apps, all extensively monitor individual movements across space, often without the users’ knowledge or permission. Within the home, a range of smart home devices such as smart meters, software-enabled thermostats and building management systems, similarly monitor activities and consumption around a house. All transactions are tracked and traced at an individual level, from clickstream and cookie data that record pathways within and between websites, to online purchases, to all online communications.

The data that Uber collects through its Android app

Data type	Data collected
Accounts log	Email log
App Activity	Name, package name, process number of activity, processed ID
App Data Usage	Cache size, code size, data size, name, package name
App Install	Installed at, name, package name, unknown sources enabled, version code, version name
Battery	Health, level, plugged, present, scale, status, technology, temperature, voltage
Device Info	Board, brand, build version, cell number, device, device type, display, fingerprint, IP, MAC address,manufacturer, model, OS platform, product, SDK code, total disk space, unknown sources enabled
GPS	Accuracy, altitude, latitude, longitude, provider, speed
MMS	From number, MMS at, MMS type, service number, to number
Net Data	Bytes received, bytes sent, connection type, interface type
Phone Call	Call duration, called at, from number, phone call type, to number
SMS	From number, service number, SMS at, SMS type, to number
Telephone Info	Cell tower ID, cell tower latitude, cell tower longitude, IMEI, ISO country code, local area code, MEID, mobile country code, mobile network code, network name, network type, phone type, SIM serial number, SIM state, subscriber ID
Wifi Connection	BSSID, IP, linkspeed, MAC addr, network ID, RSSI, SSID
Wifi Neighbors	BSSID, capabilities, frequency, level, SSID
Root Check	Root status code, root status reason code, root version, sig file version
Malware Info	Algorithm confidence, app list, found malware, malware SDK version, package list, reason code, service list, sigfile version

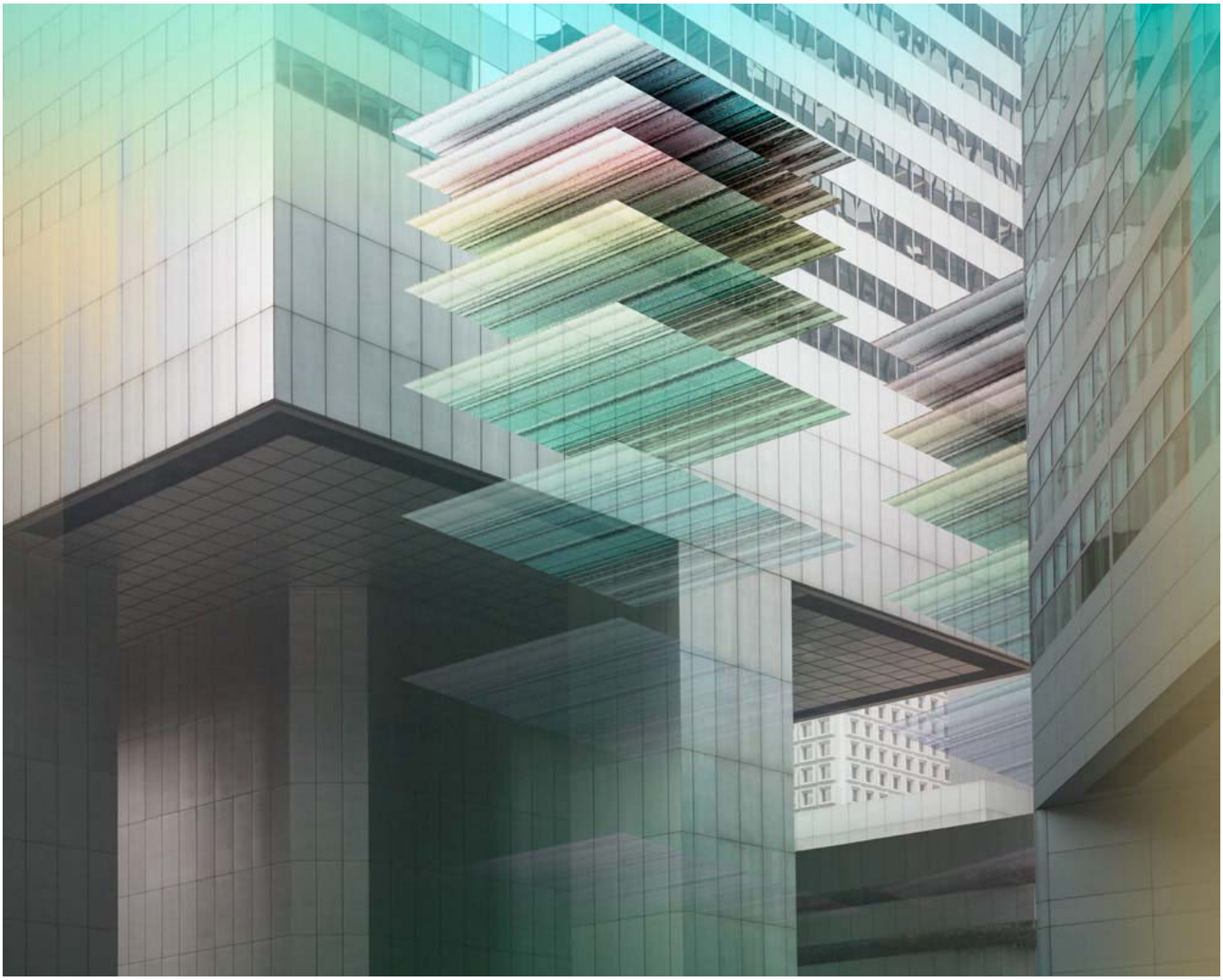
Source: Hein (2014)

Complementing all of these data are those that we voluntarily produce and share, much of it highly personal in nature relating to our thoughts, preferences, bodily performance, and movements. Consumers using a store loyalty card share their purchasing history, and those

using an online retailer might provide reviews of products or places, both revealing their preferences and lifestyle choices. Users of wearable devices, sometimes called the quantified self movement, engage in a form of sousveillance, that is self-monitoring and managing their personal health and activities, capturing consumption (e.g., food/calorie intake), physical states (e.g., blood pressure, pulse), emotional states (e.g., mood, arousal) and performance (e.g., miles walked/run/cycled, hours slept and types of sleep), all of which is shared with the technology manufacturer and often other users. In these cases, the sites through which such data are transmitted are owned by corporate enterprises whom then produce new models of capital accumulation by extracting value from them. In contrast, crowdsourced projects such as Wikipedia and Open Street Map produce collective forms of knowledge about people and places.

Collectively what all of these examples demonstrate is that the everyday practices we enact, and the places in which we live, are now deeply augmented, monitored and regulated by dense assemblages of data-enabled infrastructures and technologies on behalf of a small number of entities. The age of big data means a deluge of continuous (real-time), varied, exhaustive, fine-grained and often indexical, relational, flexible and extensional data. We are no longer simply lost in the crowd; we can be spotted, tracked and traced.

Importantly, both states and companies are generating and utilising these data, and in many cases companies are generating them for states through outsourcing contracts. The data produced has become an important multi-billion dollar commodity in their own right with vast quantities of data and derived information being rented, bought, and sold daily across a variety of markets – retail, financial, public administration, health, tourism, logistics, business intelligence, real estate, private security, political polling, and so on. Companies like Acxiom, who manage customer databases for 47 of the Fortune 100 companies, and have entered into data sharing deals with Facebook and other internet companies, claim to have created ‘360 degree views’ of up to 500 million consumers worldwide by accumulating and meshing together offline, online and mobile data into a giant databank, using these data to create detailed derived products such as profiles and predictive models (Singer 2012).



Mark Dorf, Nebulous 08, 2015

Privacy, Social Sorting, Predictive Profiling and Control Creep

What are the social consequences arising from the rush to harness the power of big urban data? Smart city technologies generate and process vast quantities of finely resolute data, which, when shared raise concerns over the demise of privacy. While multidimensional in nature, privacy generally refers to limitations concerning the accessing and disclosing of personal information about a person. Privacy is considered a basic human right, a condition that people expect and value. Indeed, it is widely considered an indispensable structural feature of liberal democratic political systems, enshrined in both national and supra-national laws. Breaching privacy can have a number of emotional effects, as well as opening up an individual to a range of harmful activities such as exposure, blackmail, appropriation (identity theft), and intrusion.

The typical response is to argue that the forfeiting of privacy is countered by many benefits —improved services and safer environments. Moreover, despite leaving an ever greater quantity of digital footprints (data they themselves leave behind) and data shadows (information about them generated by others), at present, many of the data discussed above exist largely within silos, both across city and national administrations, and across companies, and the data and systems are generally not interoperable. As a consequence, while any one data collector has a view of an individual, it is a limited field of vision. And if they do have a view of other data they are usually aggregated or metadata.

The hope of many organisations, however, is to connect silos into more comprehensive data infrastructures. This is already happening at an individual level by commercial data aggregators/brokers and policing and security services. It is certainly the ambition of many

city administrations, with many of the presentations and technologies demonstrated at the recent Smart City Expo and World Congress in Barcelona stressing the need for standardisation, the collapsing of silos to enable data from different domains to be interlinked through city command and control centers. (Much of these data concern operational systems such as lighting, transport, waste, and energy rather than individuals, though such administrations do also hold significant volumes of data about individuals and households). Centers such as the much discussed city-wide big data control room in Rio de Janeiro that combines spatial big data and public administration data from over 30 agencies, plus social media data, provide an initial blueprint, but they are quickly being followed by other cities and companies offering city operational systems. Such flattened systems open up Orwellian threats of a panopticon and taken to their logical conclusion form the perfect socio-technical assemblage for a totalitarian state—an all-seeing, all-tracking, all-reacting system that stifles dissent before it has chance to organize (which is why the technological fix to democratic street protest – extensive surveillance, algorithmic analyses, and digital kettling is so disturbing).

The argument dismissing such an Orwellian eventuality believes that democratic societies would not let anti-democratic and militaristic forms of regulation to occur, that social media and open forms of practice—open data, open access, open source, open platforms, open government—would counterbalance any censorship of mainstream media channels, that much of the data shared are anonymised and aggregated, and that companies would self-regulate to stop customer drifting away unhappy with what is happening with their data. Meanwhile, private enterprises have sought to strengthen their rights with respect to intellectual property and what they do with customer data, for example through the use of extensive and complex user agreements and political lobbying with respect to data protection laws. Indeed, there is a complex regulatory power game presently taking place around state and company surveillance, and the rights and expectations of individuals, with some arguing that it is unrealistic for people to expect or demand privacy, evidenced by the recent Pew Research report ‘The Future of Privacy’.

Until recently, given the form and resolution of data, it was difficult for data aggregators and brokers to produce individual profiles of citizens and (potential) customers *en masse*. This has changed with the data deluge, enabling them to produce predictive profiles as to the likely value or worth of an individual, or their credit risk and how likely they are to pay a certain price or be able to meet payments. The aim is to provide customers with personalized treatment, including dynamic pricing that reflects their preferences and worth, and for vendors to gain sales, increase loyalty, and reduce risk. With respect to the latter, predictive profiling is thus used to socially sort and redline populations, selecting out certain categories to receive a preferential status and marginalizing and excluding others. Through denying credit or screening career opportunities, negative profiles can haunt an individual across various domains.

Anticipatory governance is where predictive analytics are used to assess likely future behaviors or events and to direct appropriate action. A number of US police forces are now using predictive analytics to anticipate the location of future crimes and to direct police officers to increase patrols in those areas. For example, the Chicago police force produce both general area profiling to identify hotspots and guide patrols, and more specific profiling that identifies individuals within those hotspots. It achieves the latter using arrest records, phone records, social media and other data to construct the social networks of those arrested to identify who in their network is most likely to commit a crime in the future, designating them pre-criminals and visiting them to let them know that they have been flagged in their system as a potential threat (Stroud 2014). In such cases, a person’s data shadow does more than follow them; it precedes them. And knowledge that someone has been designated a pre-criminal adds yet another layer to social sorting, such as potentially being denied employment. While such systems have *prima facie* “good liberal” intentions, anticipation has consequences beyond merely preventing predicted events.

One of the key foundations of privacy and data protection laws is data minimization; that is, only data relevant to a task should be generated and such data should only be used for the purpose for which is generated. However, many technologies and the data they generate are

now being repurposed for alternative uses. For example, airline industry data and government administrative data being repurposed for profiling and assessing the security risk of passengers. Cameras deployed for regulating traffic behaviour are being repurposed for security tasks. While some of the data hoovered up Uber’s app as set out in Table 1 will be vital for the app to work, it is difficult to believe that its scope complies with the ethos of data minimization, or that its collection is in the best interest of the app user. Such repurposing, where the data generated for one set of tasks are appropriated for another, is termed control creep. Control creep removes the barriers between systems that are often presently siloed, usually for good reasons such as protecting privacy or preventing system failures in one domain affecting another, and significantly extends the power of those who gain access to additional system resources

Mark Dorf, Nebulous 05, 2015

Technocratic approaches to cities

Other concerns about the creation of smart cities include the adoption of technocratic forms of governance, the corporatisation of governance, and the creation of buggy, brittle, and hackable cities. The turn towards technical systems and algorithms to administer city regulation presumes that all aspects of a city can be measured and monitored and treated as technical problems that can be addressed through technical solutions. That is, there is a belief that complex open systems can be disassembled into neatly defined problems that can be solved or optimized through computation. Such a view is highly reductionist and

functionalist and fails to recognize the wider effects of culture, politics, policy, governance and capital in shaping city life and urban systems. It also focuses on the efficient management of the manifestations of problems, rather than solving the deep rooted structural problems underpinning them.

Further, technocratic systems tend to centralise power and decision making into a select set of administrative offices, rather than distributing power and encouraging active participation in governance. Moreover, such systems are often outsourced to companies who run them on behalf of the state, prompting anxieties over the marketisation and hollowing out of public services, that outsourcing might create a technological lock-in or corporate path dependency that beholden cities to particular systems and vendors, and cities will be straitjacketed into ‘one size fits all smart city in a box’ solutions that take little account of local cultures or political structures. Both software and cities are complex, open systems. Using software to run and manage city services and infrastructures exposes them to viruses, glitches, crashes, and security hacks. As city systems become more complicated, interconnected, and dependent on software, producing stable, robust and secure devices and infrastructures will become more of a challenge.

Regardless of the likelihood of any dystopian scenario coming to pass, it is nevertheless the case that the data revolution unfolding means that an exponentially larger amount of data are being generated about people and places by public and private institutions, that we are ever more under the gaze of continuous geosurveillance, and these data are being employed —often using opaque algorithms—to make decisions that concern our everyday lives. The privacy and freedoms we expect in liberal democracies are being changed or eroded away. At the same time, managing the complexity of cities is highly challenging and new technologies are improving the efficiency and effectiveness of city services. The key is to balance the public good and individual rights.

However, the transformations taking place are fast-paced and often too little debated or contested in the mainstream media and legislature, with disruptive technical and social innovations taking root and expanding rapidly before we have time to digest the implications or consider the need for oversight. Such thinking though is needed if we are to reap the benefits of big data and smart cities, rather than the negative consequences. How to gain the former and avoid the latter has to be worth pondering every time we interact with a digital device or traverse a city leaving a trail of data in our wake. The alternative is that smart cities are created that represent the interests of a select group of corporations, technocrats, and certain groups within society (particularly political elites and the wealthy), rather than producing ones that are in the best interests of all citizens.

Acknowledgements
Mike Pepi provided useful comments on an initial draft of this paper. The research for this paper was provided by a European Research Council Advanced Investigator Award, ‘The Programmable City’ (ERC-2012-AdG-323636).

References

Anthony, S. (2013) DARPA shows off 1.8-gigapixel surveillance drone, can spot a terrorist from 20,000 feet. ExtremeTech, 28th January 2013

Hein, B. (2014) Uber’s data-sucking Android app is dangerously close to malware. Cult of Mac, November 26th.

Marchetti, N (2012) In Portugal, A Smart City From the Ground Up. Sustainable Cities Collective. 7th June.

Singer, N. (2012a) You for Sale: Mapping, and Sharing, the Consumer Genome. New York Times, 17th June,

Stroud, M. (2014) The minority report: Chicago’s new police computer predicts crimes, but is it racist? The Verge, February 19th.

Rob Kitchin *is a professor at the National University of Ireland Maynooth and the author of* Code/Space: Software and Everyday Life *(with Martin Dodge, MIT Press, 2011) and* The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences *(Sage, 2014) and other books. He’s a regular media commentator and was the 2013 recipient of the Royal Irish Academy’s Gold Medal for the Social Sciences.*