34

GEOSURVEILLANCE AND SOCIETY

Rob Kitchin

Surveillance concerns the systematic monitoring of people, places and systems. It has long been a feature of societies, used to observe the lives and activities of citizens in order to effect law and order, secure the loyalty of subjects, monitor the efficiency and productivity of workers and provide useful information for public bodies and companies (Lyon, 2007). The nature and depth of surveillance has varied over time and space, shaped by the political ideology and economy of state governance and the development of new techniques and technologies. In the twenty-first century, the drive towards ubiquitous computing (network connections available everywhere) and pervasive computing (computation embedded into everything) has radically extended the scope and extent of surveillance. Networked digital technologies typically produce big data; that is, large volumes of real-time, exhaustive (within a system), fine-grained, uniquely indexical, relational data (Kitchin, 2014), creating a step-change in the breadth (more aspects of everyday life) and depth (fine-grained spatially and temporally) of surveillance.

Geospatial technologies are a key component of this new surveillance regime, playing a fundamental role in two key respects. First, they enable georeferenced data produced through other means (e.g., surveys, administrative systems, sensors) to be visualized, made sense of, and acted upon. Second, they perform geosurveillance, producing a rich stream of detailed, georeferenced location and movement data, most of which are big data. In other words, geospatial technologies enable the fine-grained, exhaustive monitoring and tracking of places and spatial behaviour for large populations, which was previously impossible to accomplish. For example, it is possible to track location and movement of millions of people simultaneously through a variety of networked technologies:

- controllable digital high-definition CCTV (closed circuit television) cameras (increasingly used with facial recognition software);
- smartphones and associated apps that track phone location via cell masts, GPS (global positioning system), or Wi-Fi connections;
- smart devices such as GPS-enabled fitness trackers and smart watches;
- sensor networks that capture passing phone identifiers such as MAC (media access control) addresses, enabling the tracking of movement along streets or through malls;
- public wireless networks that record actual and attempted connections by Internet-enabled digital devices (e.g., laptops, tablets, smartphones, cars);

 DOI: 10.4324/9780367855765-38

- smart card tracking that capture the scanning of barcodes/RFID chips of cards used to enter buildings or use public transport;
- vehicle tracking using Automatic Number Plate Recognition (ANPR) cameras, unique ID transponders for automated road tolls and car parking, and on-board GPS;
- other staging points, such as the use of ATMs (automatic teller machines), credit card use, metadata tagging of photos uploaded to the Internet, geotagging of social media posts;
- electronic tagging of children and parolees with GPS tracking devices;
- shared calendars that provide date, time, and location of meetings.

(Kitchin, 2015)

In addition, satellites and drones 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 (Defense Research Projects Agency) 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). The FBI (Federal Bureau of Investigation) and Department of Homeland Security have an active programme of Cessna aircraft circling many US cities daily using high-resolution video cameras, MAC address sensors, and 'augmented reality' software to superimpose other geospatial information such as property ownership onto the video feed (Aldhous and Seife, 2016).

For those that control these systems, individuals are no longer lost in the crowd; the monitoring of location and movement is pervasive, continuous, automatic, and relatively cheap. These forms of geosurveillance then are producing vast data shadows; that is, data generated by third parties about people and places. They are complemented by data footprints; that is, data produced knowingly by people about themselves, commonly known as sousveillance (Mann *et al*., 2003). For example, millions of people track their personal health by capturing their performance (e.g., miles walked/run/cycled, hours slept and types of sleep), consumption (e.g., food/calorie intake), physical states (e.g., blood pressure, pulse), and emotional states (e.g., mood, arousal) using smartphone apps and dedicated technologies (Lupton, 2016). They share their personal and family stories (via Facebook and blogs), personal thoughts (via Twitter, chat rooms and online reviews), and family photographs and videos (via Instagram and YouTube). Many of these utilize GPS to track the place of measurement and posting so that the data are georeferenced.

Geosurveillance and sousveillance are having pronounced transformative effects on three key aspects of society. They are actively reshaping the practices of governance and governmentality. They are producing new expressions of capitalism, creating new markets and means to accumulate profit. They are eroding the right to privacy and challenging civil liberties. The next three sections detail the changes occurring in three respects, followed by an illustrative discussion of their intersection in response to the COVID-19 pandemic.

Geosurveillance and governance

Surveillance technologies have long been a part of managing and governing societies. Geospatial technologies are central to contemporary governance regimes, both with respect to public space and workplaces. As well as providing a finer, more systematic grid of surveillance, these technologies are changing the nature of governance and governmentality in meaningful ways. The practices of governance are becoming more technocratic, algorithmic,

and automated. Here, governance is increasingly performed through technical, codified, data-driven systems, which have become essential architectures for managing populations, controlling, and regulating infrastructure, monitoring and directing government work, and communicating with the general public. The notion of smart cities is predicated on the use of such systems, which aim to more efficiently and effectively manage various aspects of urban life (Townsend, 2013). Geospatial technologies are a key component of such real-time governance systems, perhaps best exemplified through control rooms and associated spatial media, such as dashboards. For example, the Centro De Operacoes Prefeitura Do Rio in Rio de Janeiro, Brazil (COR) is a data-driven city operations centre that continuously monitors and manages the city and also acts as a coordinated emergency management centre. COR pulls together into a single control room real-time data streams from thirty-two agencies and twelve private concessions (e.g., bus and electricity companies), with the data used to manage and coordinate service and infrastructure delivery, maintenance, and performance (Luque-Ayala and Marvin, 2016). The centre is complemented by a virtual operations platform that enables city officials to log in from the field to access real-time information. For example, police at an accident scene can use the platform to see how many ambulances have been dispatched and their expected arrival time, and to upload additional information.

These technocratic, algorithmic systems often operate a form of 'automated management' (Dodge and Kitchin, 2007); that is, they work in automated, autonomous, and automatic ways, with systems directly regulating service delivery and citizen behaviour. In such automated systems, human involvement in their operation is limited to three levels of participation: human-in- (humans make key decisions), human-on- (algorithms make key decisions with human oversight and intervention), and human-off-the-loop (the algorithms make the key decisions) (Docherty, 2012). These systems are often concerned with regulating spatial behaviour and travel, and can rely on geospatial data. An intelligent transport system generally operates as a human-on-the-loop system, with the system automatically phasing traffic lights across the road network based on real-time data feeds, though a human controller can intervene if needed. Such automation can be contentious; for example, there is an active debate as to whether drone strikes should be administered by human-in, -on, or -off systems, with the decision to launch based on geospatial intelligence related to mobile phone location (Docherty, 2012).

In addition, governance is also becoming more predictive and anticipatory. Data have long been used to profile and segment populations, and to predict how people will behave in different scenarios and how best to manage them, but these processes have become much more sophisticated, fine-grained, widespread, and routine. The state is increasingly embracing predictive profiling and using data and algorithmic governance to make decisions about how to treat people and manage populations, allocate funding and resourcing, and deliver frontline services (Eubanks, 2017). This includes geodemographic techniques that segment and socially/spatially sort communities and places and are used to determine decisions and spatially target resources by public bodies. Many of the systems deployed use predictive modelling to assess the likelihood of particular conditions or outcomes in order to direct further attention and pre-empt situations arising. Such anticipatory governance has been a feature of air travel for a number of years, with passengers profiled regarding their security risk (Amoore, 2006). Predictive analytics has been extended into policing in general, with a number of police forces using them to anticipate the location of future crimes and to direct police officers to increase patrols in those areas, and also to identify potential suspects (Jefferson, 2018). In such predictive systems a person's data shadow does more than follow them; it precedes them. People and communities are held accountable and treated in relation to predictions rather than actual actions.

In turn, the underlying governmentality of societies is being transformed. Governmentality is the logics, rationalities, and techniques that render societies governable and enable government to enact governance (Foucault, 1991). Big data has widened, deepened, and intensified the surveillance gaze and how governance is enacted, shifting governmentality from disciplinary regimes, in which people self-regulate behaviour based on the fear of surveillance and sanction, to control regimes in which people are corralled and compelled to act in certain ways, their behaviour explicitly or implicitly steered or nudged (Deleuze, 1992). The nature of observation and management is moved from a model where an external observer is needed, to one where observation is an integral aspect of performance, with behaviour no longer adjusted in case of observation but actively reshaped (Kitchin *et al*., 2020). For example, the work of a retail checkout employee used to be monitored periodically by a supervisor on the shop floor, then via a CCTV system, and is now continually modulated by the till as they perform their work; the act of scanning is the act of surveillance. Relatedly, a transport network controlled by an intelligent transport system explicitly or implicitly nudges travel behaviour. Here, driving is modulated by traffic light sequencing and the act of driving itself becomes a site of administration (Dodge and Kitchin, 2007). In such systems, surveillance and its associated data shadow become continuous, pervasive, distributed, persistent, reactive to the subject's behaviour, but outside of the subject's control (Cohen, 2013). In more authoritarian states, geospatial technologies and geosurveillance play an active role in closely and oppressively policing and managing populations, through both disciplinary and control logics. Across all jurisdictions then, geospatial technologies are directly implicated in shifting the logics of governance in ways that have profound implications for civil liberties and citizenship.

Geosurveillance and data capitalism

Data has become a vital ingredient for leveraging value and the production and accumulation of capital, and gives rise to what Sadowski (2019) terms 'data capitalism'. That is, a form of capitalism wherein data are themselves a form of capital and not simply a commodity that can be converted into monetary value (data intrinsically have value and they produce value) and where value and profit are driven in the main or in large part by extracting value from data. Data capitalism encompasses the diverse ways data are used to accumulate profit, including optimizing systems, managing and controlling systems, modelling probabilities and planning future activities, designing and creating new products and markets, and growing the value of assets or slowing depreciation (Sadowski, 2019). A specific form of data capitalism is surveillance capitalism, which actively includes the use of geospatial technologies and their data.

Surveillance capitalism derives value and profit through the capture and monetization of data about people and places (Zuboff, 2019). In the case of geosurveillance, this involves extracting value from georeferenced data through the creation of spatial products, such as location-based targeted advertising and geodemographics (the spatial profiling and sorting of customers and places). Indeed, there is now a multi-billion-dollar market for georeferenced data globally, with a suite of specialist data companies producing, purchasing, consolidating, and linking datasets to create data products. The holdings of data brokers can be vast. In 2019, Acxiom was thought to hold data on '2.5 billion addressable consumers' in 'more than 62 countries' across more than '10,000 attributes' (Melendez and Pasternack, 2019). Equifax, a consumer credit reporting agency, has collected information on over 800 million individual consumers and over 88 million businesses worldwide (Pinchot *et al*., 2018). Experian

holds financial and purchase records for 918 million people in America, Europe, and Asia (Christl, 2017). IRI is reported to have pulled together data from more than 85,000 US retail outlets, with Nielsen collating data from 900,000 stores in more than 100 countries, and Oracle having data on billions of transactions from 1,500 chain retailers (Christl, 2017). A number of brokers specialize in location and movement data, and in spatial profiling. For example, Groundtruth, a location-focused data broker, enables companies to install their proprietary Software Development Kit into smartphone apps to deliver location-sensitive adverts, in the process collecting user location data. Their reach is about 120 million smartphone users that generate 30 billion location points a month (Smith, 2019).

In part then, extensive geosurveillance is being driven by a desire to extract value from geospatial data. As with other forms of capitalism, profit is accumulated through uneven and unequal processes of exploitation that seek to extract maximum profit at the expense of others (Sadowski, 2019). Indeed, for some surveillance capitalism is a form of modern-day colonialism in which accumulation occurs through data dispossession, with the labour of producing data rendered cheap or free, communal resources are enclosed and personal resources ensnared, and control of these exploitative relationships reside with the data extractors (Thatcher *et al.*, 2016). In other words, the users of geospatial media provide labour (e.g., clicking, swiping, typing, uploading) and data (the product of those labours) for free to those that control the means of production (Sadowski, 2019). Through this colonizing process previously non-commodified aspects of daily life are privatized and converted into commodities and a new terrain for capital investment and exchange is realized (Thatcher *et al.*, 2016).

For those providing labour and data, accumulation through data dispossession can have a profound effect on the services and opportunities extended to them, such as job offers, credit lines, insurance policy issued, tenancy approved, or what price goods and services cost, or whether a place receives targeted interventions or how it is policed (Angwin, 2014). Such profiling and sorting can work in discriminatory ways, overly misrepresenting and unfairly targeting certain groups, and reproducing and deepening inequalities by limiting life chances (Eubanks, 2017). And some companies use profiles in ways that are highly exploitative, for example offering poor deals with 'abusive terms (balloon payments, hidden fees, brutish penalty clauses) to the most vulnerable populations', or direct marketing commercial and political ads to susceptible communities (Roderick, 2014). Moreover, it can be difficult to opt out of data being captured or from data products and services. Of 212 data brokers operating in the United States examined by Angwin (2014), only 92 allowed opt-outs, and only 11 of 58 mobile location tracking businesses offered opt-outs. Moreover, opting out is not synonymous with deletion, but rather might mean omitting an individual's data from products while keeping them in the database, or only using their data in anonymous, aggregated forms (Kuempel, 2016). Whether one wants it or not then, geospatial data are being used by companies in ways that are to their advantage, but not necessarily to whom or where the data relate.

Geosurveillance, privacy, and civil liberties

Privacy – to reveal selectively oneself to the world – is a condition that many people value and expect. At a fundamental level, privacy provides a means for individuals to be able to define and present themselves; to manage what others know about them (Solove, 2006). Privacy ensures that other civil liberties, related to how individuals are treated based on what others know about them, are maintained. Privacy is understood to be a basic human right

and entitlement in most jurisdictions enshrined in national and supra-national laws. The use of geosurveillance in new regimes of governance and capitalism is having a profound effect on privacy and associated civil liberties, enabling a range of privacy and predictive privacy harms. This is particularly the case with respect to identity privacy (to protect personal and confidential data), territorial privacy (to protect personal space, objects, and property), and locational and movement privacy (to protect against the tracking of spatial behaviour) (Kitchin, 2016).

The consensus of academics, lawyers, and civil liberties groups concerned about privacy is that extensive surveillance through networked, big data technologies has placed enormous strain on present legal frameworks in Europe and North America. In both geographic spheres, privacy legal provisions draw extensively on the OECD's (Organization for Economic Co-operation and Development) fair information practice principles (FIPPs). These prioritize personal rights regarding the generation, use, and disclosure of personal data, and place obligations on data controllers and processors (Solove, 2013). Other jurisdictions have their own approaches (see DLA Piper, 2019) or have limited legal protections; for example, only eight out of 55 Sub-Saharan African countries had data protection legislation in place in 2013 (Greenleaf, 2013).

In the big data age, FIPPs are being challenged and undermined in several ways. A key premise of big data is that they are repurposed so that additional value can be leveraged. Repurposing runs counter to data minimization, one of the key FIPPs. Data minimization stipulates that data controllers and processors should only generate data necessary to perform a particular task, that the data are only retained for as long as they are required to perform that task, and that the data generated should only be used for this task (Tene and Polonetsky, 2012). The solution has been to repackage personally identifiable information through de-identifying them or creating derived data that is exempt from the provisions. However, unless carefully undertaken it is possible to re-identify data through various techniques. One example relating to geospatial data concerns a dataset released by the New York City Taxi and Limousine Commission in 2013 relating to 173 million individual cab rides. The taxi drivers' medallion numbers were anonymized but were quickly de-identified, enabling information related to pickup and drop-off times, locations, fare and tip amounts to be tied to specific drivers, and to infer their home address, income, and religion (by if they took breaks to pray at set times). By combining this dataset with other public information, like celebrity blogs, it was possible to determine home addresses and where and who was visited (Metcalf and Crawford, 2016).

FIPPs do not relate to predictive privacy harms or group privacy harms. Predictive modelling can generate inferences about an individual and places that reinforce or create stigma and harm (Crawford and Schultz, 2014). For example, tracking data that reveals a person frequents gay bars, leading to the inference that the person is likely to gay, could be harmful if shared inappropriately. Yet, as no data about sexuality has been directly collected it is exempt from FIPPs provisions. Similarly, co-proximity and co-movement with others can be used to infer political, social, and/or religious affiliation, potentially revealing membership of particular groups (Leszczynski, 2017). Moreover, at present, approaches to privacy focus almost exclusively on individual interests and personal harm (Taylor *et al*., 2017). However, this individual focus fails to recognize that aggregated data relating to groups can lead to group privacy harms by enabling group members to be targeted and treated with minimal protections (Rainie *et al*., 2019). This is particularly problematic with respect to marginalized groups who are already collectively victimized through actions that indiscriminately target members.

Conclusion

Geospatial technologies undoubtedly have many productive uses and make positive contributions to society and economy. They are also key agents of geosurveillance and have troubling effects with respect to governance, capitalism, and civil liberties. The tension between productive uses and troubling effects has been well illustrated through the use of geospatial technologies and georeferenced data to try to limit the spread of COVID-19 (Kitchin, 2020; Taylor *et al*., 2020). A number of new and existing technologies designed to restrict movement (smartphone apps, facial recognition and thermal cameras, biometric wearables, smart helmets, drones, and predictive analytics) were rapidly developed or re-orientated for contact tracing, quarantine enforcement, travel permission, social distancing/movement monitoring, and symptom tracking.

In South Korea, the government utilized surveillance camera footage, smartphone location data, and credit card purchase records to track positive cases and their contacts (Singer and Sang-Hun, 2020). Singapore quickly launched TraceTogether, a Bluetooth-enabled app that detects and stores the details of nearby phones to enable contact tracing, with dozens of other countries launching similar apps shortly after (Taylor *et al*., 2020). Moscow authorities rolled out an app system to pre-approve journeys and routes (Ilyushina, 2020). Taiwan deployed a mandatory phone-location tracking system to enforce quarantines (Timberg and Harwell, 2020). In some parts of China citizens were required to scan QR codes when accessing public spaces and transit systems to verify their infection status and gain permission (Goh, 2020). A number of companies offered, or actively undertook, repurposing of their platforms and data as a means to help tackle the virus. In Germany, Deutsche Telekom provided aggregated, anonymized information to the government on peoples' movements; likewise, Telecom Italia, Vodafone and WindTre did the same in Italy (Pollina and Busvine, 2020). Palantir monitored and modelled the spread of the disease to predict the required health service response for the Center for Disease Control in the US and the National Health Service in the UK (Hatmaker, 2020), and a number of cyber-intelligence companies such as NSO Group, Cellebrite, Intellexa, Verint Systems, and Rayzone Group offered their people tracking services to governments (Schectman *et al*., 2020).

For many politicians, policy makers, and citizens the use of these surveillance technologies was legitimated by the need to contain the virus and save lives, regardless of their effects on civil liberties. For others, their deployment and the extensive geosurveillance enacted was highly problematic, raising a number of civil liberties and political economy concerns. Much of the public debate focused on privacy, since the technologies demand fine-grained knowledge about location, movement, social networks, and health status, and what else might be done with these data (Taylor *et al*., 2020). However, there were also concerns relating to governance given the technologies socially and spatially sorted people, redlining who could and could not mix, move and access spaces and services, and the extent to which these technocratic measures would creep into other domains and persist after the pandemic (in the same way heightened security measures persisted after 9/11). The Chinese government indicated that some of its intervention systems will remain in place post-pandemic, and although the Singapore government assured citizens that TraceTogether would only be used for contact tracing, a few months later it changed the terms to include movement data being available to the police for criminal matters (Mohan, 2021). In addition, there were worries about the lack of due process, oversight, and the right to redress and to opt out from systems (McDonald, 2020). Others were troubled that pursuing surveillance-based solutions in collaboration with industry legitimated and normalized the methods and logics of surveillance

capitalism, while at the same time opening up sensitive public health data to private interests (Taylor *et al*., 2020). Moreover, the use of privately generated geosurveillance by states enabled the 'covidwashing' surveillance practices while simultaneously opening up new markets (Kitchin, 2020).

Despite arguments that public health trumped civil liberty concerns, when pressured by civil liberties organizations governments were able to ensure that appropriate safeguards were put in place to protect civil liberties (e.g., anonymization, encryption, not sharing data and deleting after two weeks, discontinuation at end of pandemic, publishing code and data protection assessments) while still being able to use the technologies for the purpose intended. In other words, it was proven that public health interventions could be enacted while preserving civil liberties when sufficient public pressure is applied, and the same is undoubtedly the case with respect to other uses of geospatial technologies. What this concluding discussion highlights is that there are a number of ethical and data justice issues relating to the use of geospatial technologies and the vast volumes of data they produce. These issues pose numerous moral dilemmas and inconvenient truths, which are often avoided or glossed over by the geospatial community. While some, notably within the Critical GIS community, do try to explore such issues and moderate their practices, it is clear that wider normative debates about geosurveillance are still required.

Acknowledgements

This chapter draws heavily on previously published work, in particular Kitchin (2015), Kitchin (2016), Kitchin (2020), and Kitchin *et al*. (2020). The research was supported by the European Research Council (grant ERC-2012-AdG-323636) and Science Foundation Ireland (grant 15/IA/3090).

References

Aldhous, P. and Seife, C. (2016) "Spies in the Sky: See Maps Showing Where FBI Planes Are Watching From Above" *BuzzFeed* (6th April) Available at: https://www.buzzfeednews.com/article/peteraldhous/spies-in-the-skies.

Amoore, L. (2006) "Biometric Borders: Governing Mobilities in the War on Terror" *Political Geography* 25 pp.336–351.

Angwin, J. (2014) *Dragnet Nation* New York: St Martin's Press.

Anthony, S. (2013) "DARPA Shows Off 1.8-Gigapixel Surveillance Drone, Can Spot a Terrorist from 20,000 Feet" *ExtremeTech* (28 January) Available at: https://www.extremetech.com/extreme/-146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet.

Christl, W. (2017) *Corporate Surveillance in Everyday Life* Vienna: Cracked Labs.

Cohen, J.E. (2013) "What is Privacy For?" *Harvard Law Review* 126 pp.1904–1933.

Crawford, K. and Schultz, J. (2014) "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms" *Boston College Law Review*, 55 pp.93–128.

Deleuze, G. (1992) "Postscript on the Societies of Control" In Szeman, I. and Kaposy, T. (Eds) (2010) *Cultural Theory: An Anthology* John Wiley & Sons, pp.139–142.

DLA Piper (2019) "Data Protection Laws of the World" Available at:https://www.dlapiperdataprotection.com/#handbook/world-map-section.

Docherty, B. (2012) *Losing Humanity: The Case Against Killer Robots* New York: Human Right Watch, New York.

Dodge, M. and Kitchin, R. (2007) "The Automatic Management of Drivers and Driving Spaces" *Geoforum* 38 (2) pp.264–275.

Eubanks, V. (2017) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* New York: St Martin's Press.

Foucault, M. (1991) "Governmentality" In Burchell, G., Gordon, C. and Miller, P. (Eds) *The Foucault Effect: Studies in Governmentality* Chicago: University of Chicago Press, pp.87–104.

Goh, B. (2020) "China Rolls Out Fresh Data Collection Campaign to Combat Coronavirus" *Reuters* (26th February) Available at: https://www.reuters.com/article/us-china-health-data-collection/china-rolls-outfresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW.

Greenleaf, G. (2013) "Scheherazade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" *Journal of Law, Information & Science* 23 (1) pp.4–49.

Hatmaker, T. (2020) "Palantir Provides COVID-19 Tracking Software to CDC and NHS, Pitches European Health Agencies" *TechCrunch* (1st April) Available at: https://techcrunch.com/2020/04/01/palantircoronavirus-cdc-nhs-gotham-foundry/.

Ilyushina, M. (2020) "Moscow Rolls Out Digital Tracking to Enforce Lockdown: Critics Dub it a 'Cyber Gulag'" *CNN* (14th April) Available at: https://edition.cnn.com/2020/04/14/world/-moscow-cyber-tracking-qrcode-intl/index.html.

Jefferson, B.J. (2018) "Predictable Policing: Predictive Crime Mapping and Geographies of Policing and Race" *Annals of the American Association of Geographers* 108 (1) pp.1–16.

Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* London: Sage.

Kitchin, R. (2015) "Spatial Big Data and the Era of Continuous Geosurveillance" *DIS Magazine* Available at: http://dismagazine.com/issues/73066/rob-kitchin-spatial-big-data-and-geosurveillance/.

Kitchin, R. (2016) *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security* Dublin:,Data Protection Unit, Department of the Taoiseach.

Kitchin, R. (2020) "Civil Liberties or Public Health, or Civil Liberties and Public Health? Using Surveillance Technologies to Tackle the Spread of COVID-19" *Space and Polity* 24 (3) pp.362–381 DOI: 10.1080/13562576.2020.1770587.

Kitchin, R., Coletta, C. and McArdle, G. (2020) Governmentality and urban control. In Willis, K. and Aurigi, A. (eds) *The Companion to Smart Cities*. Routledge, London, pp. 109–122.

Kuempel, A. (2016) "The Invisible Middlemen: Critique and Call for Reform of the Data Broker Industry" *Northwestern Journal of International Law & Business* 36 (1) pp.207–234.

Leszczynski, A. (2017) "Geoprivacy" In Kitchin, R., Lauriault, T. and Wilson, M. (Eds) *Understanding Spatial Media* London: Sage, pp.239–248.

Lupton, D. (2016) *The Quantified Self* Cambridge: Polity.

Luque-Ayala, A. and Marvin, S. (2016) "The Maintenance of Urban Circulation: An Operational Logic of Infrastructural Control" *Environment and Planning D: Society and Space* 34 (2) pp.191–208.

Lyon, D. (2007) *Surveillance Studies: An Overview* Cambridge: Polity.

Mann, S., Nolan, J. and Wellman, B. (2003) "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments" *Surveillance and Society* 1 (3) pp.331–355.

McDonald, S. (2020) "The Digital Response to the Outbreak of COVID-19" *Centre for International Governance Innovation* (30th March) Available at: https://www.cigionline.org/articles/digital-response-outbreak-covid-19.

Melendez, S. and Pasternack, A. (2019) "Here Are the Data Brokers Quietly Buying and Selling Your Personal Information" *The Fast Company* (2nd March) Available at: https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

Metcalf, J. and Crawford, K. (2016) "Where Are Human Subjects in Big Data Research? The Emerging Ethics Divide" *Big Data & Society* 3 (1) pp.1–14.

Mohan, M. (2021) "Singapore Police Force Can Obtain Tracetogether Data for Criminal Investigations" *CNA* (4th January) Available at: https://www.channelnewsasia.com/news/singapore/singapore-police-force-can-obtain-tracetogether-data-covid-19-13889914.

Pinchot, J., Chawdhry, A.A. and Paullet, K. (2018) "Data Privacy Issues in the Age of Data Brokerage: An Exploratory Literature Review" *Issues in Information Systems* 19 (3) pp.92–100.

Pollina, E. and Busvine, D. (2020) "European Mobile Operators Share Data for Coronavirus Fight" *Reuters* (18th March) Available at: https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/europeanmobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2.

Rainie, S.C., Kukutai, T., Walter, M., Figueroa-Rodríguez, O.L., Walker, J. and Axelsson, P. (2019) "Issues in Open Data: Indigenous Data Sovereignty" In Davies, T., Walker, S., Rubinstein, M. and Perini, F. (Eds) *The State of Open Data: Histories and Horizons* Cape Town and Ottawa: African Minds and International Development Research Centre, pp.300–319.

Roderick, L. (2014) "Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry" *Critical Sociology* 40 (5) pp.729–746.

Sadowski, J. (2019) "When Data is Capital: Datafication, Accumulation, and Extraction" *Big Data & Society* 5 (1) pp.1–12.

Schectman, J., Bing, C. and Stubbs, J. (2020) "Cyber-intel Firms Pitch Governments on Spy Tools to Trace Coronavirus" *Reuters* (28th April) Available at: https://www.reuters.com/article/us-health-coronavirusspy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-tracecoronavirus-idUSKCN22A2G1.

Singer, N. and Sang-Hun, C. (2020) "As Coronavirus Surveillance Escalates, Personal Privacy Plummets" *New York Times* (23rd March) Available at: https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

Smith, H. (2019) "Monetizing Movement: Groundtruth" In Graham, M., Kitchin, R., Mattern, S. and Shaw, J. (Eds) *How to Run a City Like Amazon, and Other Fables* Oxford: Meatspace Press, pp.570–605.

Solove, D.J. (2006) "A Taxonomy of Privacy" *University of Pennsylvania Law Review* 154 (3) pp.477–560.

Solove, D. (2013) "Privacy Management and the Consent Dilemma" *Harvard Law Review* 126 pp.1880–1903.

Taylor, L., Floridi, L. and van der Sloot, B. (2017) "Introduction: A new perspective on privacy" In Taylor, L., Floridi, L. and van der Sloot, B. (Eds) *Group Privacy: New Challenges of Data Technologies* Cham, Switzerland: Springer, pp.1–12.

Taylor, L., Sharma, G., Martin, A. and Jameson, S. (2020) *Data Justice and Covid-19: Global Perspectives* London: Meatspace Press.

Tene, O. and Polonetsky, J. (2013) "Big Data for All: Privacy and User Control in the Age of Analytics" *Northwestern Journal of Technology and Intellectual Property* 11 (5) pp.240–273.

Thatcher, J., O'Sullivan, D. and Mahmoudi, D. (2016) "Data Colonialism Through Accumulation by Dispossession: New Metaphors for Daily Data" *Environment and Planning D: Society and Space* 34 (6) pp.990–1006.

Timberg, C. and Harwell, D. (2020) "Government Efforts to Track Virus Through Phone Location Data Complicated by Privacy Concerns" *Washington Post* (19th March) Available at: https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/.

Townsend, A. (2013) *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: W.W. Norton & Co.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* New York: Profile Books.