PHILOSOPHICAL TRANSACTIONS A

rsta.royalsocietypublishing.org

Research

Cite this article: Kitchin R. 2016 The ethics of smart cities and urban science. *Phil. Trans. R. Soc. A* **374**: 20160115.
http://dx.doi.org/10.1098/rsta.2016.0115

Accepted: 13 July 2016

One contribution of 15 to a theme issue 'The ethical impact of data science'.

Subject Areas:
computer modelling and simulation, software

Keywords:
big data, smart cities, urban science, dataveillance, privacy, ethics

Author for correspondence:
Rob Kitchin
e-mail: rob.kitchin@nuim.ie

The ethics of smart cities and urban science

Rob Kitchin

National Institute for Regional and Spatial Analysis, National University of Ireland Maynooth, County Kildare, Ireland

RK, 0000-0003-4458-7299

Software-enabled technologies and urban big data have become essential to the functioning of cities. Consequently, urban operational governance and city services are becoming highly responsive to a form of data-driven urbanism that is the key mode of production for smart cities. At the heart of data-driven urbanism is a computational understanding of city systems that reduces urban life to logic and calculative rules and procedures, which is underpinned by an instrumental rationality and realist epistemology. This rationality and epistemology are informed by and sustains urban science and urban informatics, which seek to make cities more knowable and controllable. This paper examines the forms, practices and ethics of smart cities and urban science, paying particular attention to: instrumental rationality and realist epistemology; privacy, datafication, dataveillance and geosurveillance; and data uses, such as social sorting and anticipatory governance. It argues that smart city initiatives and urban science need to be re-cast in three ways: a re-orientation in how cities are conceived; a reconfiguring of the underlying epistemology to openly recognize the contingent and relational nature of urban systems, processes and science; and the adoption of ethical principles designed to realize benefits of smart cities and urban science while reducing pernicious effects.

This article is part of the themed issue 'The ethical impact of data science'.

1. Urban big data and smart cities

For as long as data have been generated about cities, various kinds of data-informed urbanism have been occurring; that is, data have been used as the evidence base for formulating urban policies, programmes and plans, to track their effectiveness and to model and

THE ROYAL SOCIETY PUBLISHING

simulate future development. The data employed have typically been sampled, generated on a one-off or occasional basis, and are limited in scope. Such data include censuses, household, transport, environment and mapping surveys, and commissioned interviews and focus groups, complemented with various forms of public administration records. In general, these data are analysed at the aggregate level and provide snapshots of cities at particular moments.

Increasingly, these datasets are being supplemented with new forms of urban big data. Big data have fundamentally different properties to traditional 'small' datasets, being generated and processed in real time, exhaustive in scope and having fine resolution [1]. Rather than data being derived from a travel survey with a handful of city dwellers during a specific time period, transport big data consist of a continual survey of every traveller: for example, collecting *all* the tap-ins and tap-outs of Oyster cards on the London Underground, or using automatic number plate recognition (ANPR)-enabled cameras to track *all* vehicles, or using sensors to monitor the mobile phone MAC addresses to track *all* pedestrians with a phone.

This transformation from slow and sampled data to fast and exhaustive data has been enabled by the roll-out of a raft of new networked, digital technologies embedded into the fabric of urban environments that underpin the drive to create smart cities. Such technologies include digital cameras, sensors, transponders, meters, actuators, GPS and transduction loops that monitor various phenomena and continually send data to an array of control and management systems, such as city operating systems, centralized control rooms, intelligent transport systems, logistics management systems, smart energy grids and building management systems that can process and respond in real time to the data flow [2–4]. In addition, a multitude of smartphone apps and sharing economy platforms generate a range of real-time location, movement and activity data. In other words, there has been a marked intensification of what has been termed 'dataficiation' [5]; that is, a radical expansion in the volume, range and granularity of the data being generated about people and places [4,6]. As the data are digital and organized and stored in digital databases, they are easily conjoined and shared and highly suited to examination using data analytics.

The result is a vast deluge of real-time, fine-grained, contextual and actionable data, which are routinely generated about cities and their citizens by a range of public and private organizations, including:

— utility companies (use of electricity, gas and water);
— transport providers (location/movement, travel flow);
— mobile phone operators (location/movement, app use and behaviour);
— travel and accommodation websites (reviews, location/movement and consumption);
— social media sites (opinions, photos, personal information and location/movement);
— crowdsourcing and citizen science (maps, e.g. OpenStreetMap; local knowledge, e.g. Wikipedia; weather, e.g. Wunderground);
— government bodies and public administration (services, performance and surveys);
— financial institutions and retail chains (consumption and location);
— private surveillance and security firms (location and behaviour);
— emergency services (security, crime, policing and response); and
— home appliances and entertainment systems (behaviour and consumption).

While some of these data are generated by local authorities and state agencies, much of the data are considered a private asset. The latter are generally closed in nature, though they might be shared with third party vendors (such as city authorities, often for a fee) or researchers (using a licence). In some cases, they are open in nature, often on a limited basis (through data infrastructures or APIs).

These urban big data, it is contended, produce a highly granular, longitudinal, whole system understanding of a city system or service and enable city systems to be managed in real time. Data about how a system is performing can be streamed back from across the infrastructure, analysed, and appropriate responses returned. For example, data on traffic flow generated by sensors, transduction loops, cameras and transponders in public vehicles (such as buses or city

vehicles), or through social media such as Waze, can be generated on a real-time basis, fed back to a control room where software and analysts can monitor traffic levels and alter traffic light sequencing and road speeds to try and maintain traffic flow. Moreover, it is possible to determine patterns of travel across times of the day, days of the week, and seasons, and to do this for all nodes on the network (e.g. junctions, bus stops, sensor locations). Further, the data can be used to create and improve models and simulations to guide future urban development. For example, to simulate what might happen to travel patterns or land values by closing a road or siting a new hospital on the network.

The consequence of the emerging data deluge is that data-informed urbanism is increasingly being complemented and replaced by data-driven urbanism (the mode of production of smart cities) and this is changing how we know, plan and govern cities, both within particular domains (e.g. transport, environment, lighting, waste management, etc.) and across them [7–9]. Indeed, one of the consequences of data-driven urbanism is that city systems and infrastructures are becoming much more tightly interlinked and integrated. For example, urban operating systems explicitly link together multiple smart city technologies to enable greater coordination of city systems. Similarly, urban operating centres and urban dashboards attempt to draw together and interlink urban big data to provide synoptic city intelligence [8]. For example, the Centro De Operacoes Prefeitura Do Rio is a purpose built urban operations centre, staffed by 400 professional workers [10], which draws together real-time data streams from 30 agencies, including traffic and public transport, municipal and utility services, emergency services, weather feeds, social media and information sent in by the public via phone, Internet and radio. This is complemented by a virtual operations platform accessible by mobile devices that enable city officials to log-in from the field to access and upload real-time information [11]. In the centre a team of analysts, aided by various data analytics software, process, visualize, analyse and monitor the vast deluge of live service data using them for real-time decision-making and problem solving. The result is a new form of highly responsive urban governance in which big data systems are prefiguring and setting the urban agenda and are influencing and controlling how city systems respond and perform.

2. Urban science/informatics

The development of urban big data and data-driven urbanism are informed by and sustain data science practised within the fields of urban science (a computational modelling and simulation approach to understanding, explaining and predicting city processes) and urban informatics (an informational and human–computer interaction approach to examining and communicating urban processes). Indeed, there is a strong recursive relationship between data-driven urbanism and urban science/informatics, with the former providing the raw material and applied domain and the latter providing fundamental ideas and the key tools to enact city analytics and data-driven decision-making. Urban science and urban informatics both forward a computational understanding of city systems and seek to address the two fundamental challenges posed by urban big data: (i) how to handle and make sense of millions or billions of observations that are being generated on a dynamic basis [3] and (ii) how to translate the insight derived into new urban theory (fundamental knowledge) and actionable outcomes (applied knowledge) [12–14].

Urban science/informatics, it is posited, offers the potential for urban knowledge that has greater breadth, depth, scale and timeliness, and is inherently longitudinal, in contrast with that derived from longer standing, more traditional urban studies [3,15]. With respect to the former, the emphasis has been on the development of new data analytics that utilize machine learning techniques designed to process and analyse enormous datasets, such as data mining and pattern recognition, data visualization and visual analytics, statistical analysis, and prediction, simulation and optimization modelling [4,13,16]. These techniques are largely in their infancy given that traditional statistical methods were designed to perform data-scarce science; that is, identify significant relationships from small, clean sample sizes with known properties [3]. Nonetheless, significant progress has been made within computer science, data science and information science with respect to handling and extracting insights from big data and these have been utilized

within urban science/informatics. Further, there is a longer legacy of scientific and informatics approaches to cities that provide a bedrock of knowledge. This legacy is rooted in quantitative geography and urban modelling [17,18], digital mapping and geographic information systems [19,20], and in urban cybernetics theory and practice [21].

These approaches adopt a realist epistemology that supposes the existence of an external reality which operates independently of an observer and which can be objectively and accurately measured, tracked, statistically analysed, modelled and visualized to reveal the world as it actually is. In other words, urban data can be unproblematically abstracted from the world in neutral, value-free and objective ways and are understood to be essential in nature; that is, fully representative of that which is being measured (they faithfully capture its essence and are independent of the measuring process) [22]. And these data when analysed in similarly objective ways reveal the truth about and a 'God's eye' view of cities. As such, they promote an instrumental rationality that underpins the notion that cities can be steered and managed through a set of data levers and analytics and that urban issues can be solved through a range of technical solutions [8,23,24].

Such a framing led to initial spatial and urban science to be roundly criticized within the social sciences for being too closely aligned with positivist thinking, being reductionist, mechanistic, atomizing, essentialist, deterministic and parochial, collapsing diverse individuals and complex, multidimensional social structures and relationships to abstract data points and universal formulae and laws [25], and producing policy interventions that not only failed to live up to their promises but also did much damage to city operations [26]. These approaches also wilfully ignored the metaphysical aspects of human life and the role of politics, ideology, social structures, capital and culture in shaping urban relations, governance and development [27]. Consequently, they fail to recognize that cities are complex, multifaceted, contingent, relational systems, full of contestation and wicked problems that are not easily captured or steered, and that urban issues are often best solved through political/social solutions and citizen-centred deliberative democracy, rather than technocratic forms of governance [8,28].

As such, computational and scientific approaches to cities produce a limited and limiting understanding of how cities work (foreclosing what kinds of questions can be asked and how they can be answered) and how they should be managed (foreclosing other forms of urban governance and other forms of knowledge, such as phronesis, knowledge derived from practice and deliberation, and metis, knowledge based on experience [29]). These critiques undoubtedly still hold, though advocates of computational social and urban science counter that in the age of big data the variety, exhaustivity, resolution and relationality of data, plus the growing power of computation and new data analytics, address some of the criticism, especially those of reductionism and universalism, by providing more finely grained, sensitive, and nuanced analysis that can take account of context and contingency [1].

While current urban science undoubtedly draws on positivistic ideas, notably that emanating within social physics which seeks to identify the social determinates and 'laws' of cities while largely ignoring the longer canon and critique [30,31]—and is open to the same criticisms as earlier manifestations—it should be noted that its approach is shaped by two more recent epistemological positions [1]. The first is a form of inductive empiricism in which it is argued that through data analytics urban big data can speak for themselves free of theory or human bias or framing. Such an approach is best exemplified by Anderson [32] who argues that 'the data deluge makes the scientific method obsolete' and that within big data studies 'correlation supersedes causation, and science can advance even without coherent models, unified theories, or really any mechanistic explanation at all'. In other words, rather than being guided by theory, the data can be wrangled through hundreds of algorithms to discover the most salient factors with regards to a particular phenomenon. The second is data-driven science that seeks to hold to the tenets of the scientific method, but seeks to generate hypotheses and insights 'born from the data' rather than 'born from the theory' [33, p. 613]. It uses guided knowledge discovery techniques to mine the data to identify potential hypotheses, before a traditional deductive approach is employed to test their validity. It is contended that data-driven science will become the new dominant

mode of scientific method in the big data age because its epistemology is suited to exploring, extracting value, and making sense of massive, interconnected datasets; it extracts additional, valuable insights that traditional knowledge-driven science would fail to generate and it produces more holistic and extensive models and theories of entire complex systems rather than elements of them [16,33]. Both approaches are evident in urban science/informatics, with a preference on the latter.

3. The ethics of data-driven urbanism and urban science

The unfolding deluge of fast, exhaustive, indexical data, the wide-scale attempts to extract value from and make sense of such data, and the desire to translate actionable data and data analytics into modes of data-driven management and governance and commercial products raise a number of ethical issues concerning privacy, datafication, dataveillance and geosurveillance, and data uses such as social sorting and anticipatory governance. The rest of the paper examines these issues and considers how data-driven urbanism and urban science might seek to address the concerns raised. The argument forwarded is not that we need to abandon the creation of smart cities and scientific and informatics approaches to understanding cities, but rather that such initiatives need to be re-imagined and re-cast in ways which seek to minimize their pernicious effects, and lay bare instrumental rationality and epistemology, and recognize the value of other ways of knowing and doing.

(a) Datafication and privacy

Privacy—to selectively reveal oneself to the world—is considered a basic human right in many jurisdictions (particularly democratic states), enshrined in national and supra-national laws in various ways. How privacy is understood both as an everyday and legal concept, however, varies between cultures and contexts. In general terms, privacy debates concern acceptable practices with regards to accessing and disclosing personal and sensitive information about a person [34]. Such sensitive information can relate to a number of a personal facets and domains creating a number of inter-related privacy forms including [35,36]:

— identity privacy (to protect personal and confidential data);
— bodily privacy (to protect the integrity of the physical person);
— territorial privacy (to protect personal space, objects and property);
— locational and movement privacy (to protect against the tracking of spatial behaviour);
— communications privacy (to protect against the surveillance of conversations and correspondence); and
— transactions privacy (to protect against monitoring of queries/searches, purchases, and other exchanges).

As Solove [37] details, these forms of privacy can be threatened and breached through a number of what are normally understood as unacceptable practices, each of which produces a different form of harm (table 1). Smart city technologies, data-driven urbanism and urban science create a number of potential privacy harms for five reasons, each of which also raises significant challenges to existing approaches to protecting privacy (privacy laws and fair information practice principles).

(i) Datafication, dataveillance and geosurveillance

Increased datafication means that people are now subject to much greater levels of intensified scrutiny as more and more aspects of their daily lives are captured as data. Indeed, the pervasiveness of digitally mediated transactions and surveillance, plus the increasing use of unique identifiers and personally identifiable information (PII) to access services (e.g. names, usernames, passwords, account numbers, addresses, emails, phone details, credit card numbers,

Table 1. A taxonomy of privacy breaches and harms. Source: compiled from [37].

domain	privacy breach	description
information collection	surveillance	watching, listening to, or recording of an individual's activities
	interrogation	various forms of questioning or probing for information
information processing	aggregation	the combination of various pieces of data about a person
	identification	linking information to particular individuals
	insecurity	carelessness in protecting stored information from leaks and improper access
	secondary use	use of information collected for one purpose for a different purpose without the data subject's consent
	exclusion	failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data
information dissemination	breach of confidentiality	breaking a promise to keep a person's information confidential
	disclosure	revelation of information about a person that impacts the way others judge her character
	exposure	revealing another's nudity, grief, or bodily functions
	increased accessibility	amplifying the accessibility of information
	blackmail	threat to disclose personal information
	appropriation	the use of the data subject's identity to serve the aims and interests of another
	distortion	dissemination of false or misleading information about individuals
invasion	intrusion	invasive acts that disturb one's tranquillity or solitude
	decisional interference	incursion into the data subject's decisions regarding her private affairs

smart card ID, licence plates and faces), means that it is all but impossible to live everyday lives without leaving digital footprints (traces we leave ourselves) and shadows (traces captured about us) [38]. The result is the deepening of dataveillance and, in the case of the smart city, geosurveillance. Dataveillance is a mode of surveillance enacted through generating, sorting and sifting datasets in order to identify, monitor, track, regulate, predict and prescribe [39,40]. Geosurveillance is the tracking of location and movement of people, vehicles, goods and services and the monitoring of interactions across space [41].

With regards to the latter, up until relatively recently tracking the movement of individuals was a slow, labour-intensive, partial and difficult process. The only way to track the location and movements of an individual were to follow them in person and to quiz those with whom they interacted. As a result, people's movement was undocumented unless there was a specific reason to focus on them through the deployment of costly resources. Even if a person was tracked, the records tended to be partial, bulky, difficult to cross-tabulate, aggregate and analyse, and expensive to store. A range of smart technologies has transformed geo-location tracking to a situation where the monitoring of location is pervasive, continuous, automatic and relatively cheap and it is relatively easy to construct travel profiles and histories.

For example, many cities are saturated with remote controllable digital CCTV cameras that can zoom, move and track individual pedestrians. In addition, large parts of the road network and the movement of vehicles are surveyed by traffic, red-light, congestion and toll cameras. Analysis and interpretation of CCTV footage is increasingly aided by facial, gait and ANPR using machine vision algorithms. Several police forces in cities in the UK have rolled out CCTV facial recognition programmes [42,43], as have cities in the USA, including New York and Chicago (each with over 24 000 cameras) [44]. ANPR cameras are installed in many cities for monitoring traffic flow, but also for administrating traffic violations such as the non-payment of road tolls and congestion charging. There are an estimated 8300 ANPR cameras across the UK capturing 30 million number plates each day [45].

In a number of cities, sensor networks have been deployed across street infrastructure such as bins and lampposts to capture and track phone identifiers such as MAC addresses. In London, Renew installed such sensors on 200 bins, capturing in a single week in 2014 identifiers from over four million devices and tracking these as they moved from bin to bin [46]. The company reported that they could measure the proximity, speed and manufacturer of a device and track the stores individuals visited, how long they stayed there, and how loyal customers are to particular shops. The same technology is also used within malls and shops to track shoppers, sometimes linking with CCTV to capture basic demographic information such as age and gender [47]. Similarly, some cities have installed a public wifi mesh, which can capture the IDs of devices that access the network and then track them between wifi points.

Many buildings use smart card tracking, with unique identifiers installed either through barcodes or embedded radiofrequency identification chips. Cards are used for access control to different parts of the building and to register attendance, but can also be used as an electronic purse to pay for items within the facility [48]. Smart cards are also used to access and pay for public transport, such as the Oyster Card in London. Each reading of the card adds to the database of movement across a city.

Smartphones continuously communicate their location to telecommunications providers, either through the cell masts they connect to, or by sending of GPS coordinates, or their connections to wifi hotspots. Likewise, smartphone apps can access and transfer such information and also share them to third parties. With respect to the latter, the *Wall Street Journal* in 2011 [49] details that 25 out 50 iPhone apps, and 21 of 50 Android apps transmitted location data to a third party other than the app developer [50]. New vehicles are routinely fitted with GPS that enables the on-board computers to track location, movement, and speed. Active GPS tracking is commonly used in fleet management to track goods vehicles, public transport and hire cars, or to monitor cars on a payment plan to ensure that they can be traced and recovered in cases of default. Moreover, cars are increasingly being fitted with unique ID transponders that are used for the automated operation and payment of road tolls and car parking.

Selected populations—such as people on probation, prisoners on home leave, people with dementia, children—are being electronically tagged to enable tracking. Typically, this is done using a GPS-enabled bracelet that periodically transmits location and status information via a wireless telephone network to a monitoring system. In other cases, it is possible to install tracker apps onto a phone (of say children) so the phone location can be tracked, or to buy a family tracking service from telecoms providers [48]. There are also many other staging points where we might leave an occasional trace of our movement and activities, such as using ATMs, or using a credit card in a store, or checking a book out of a library. Another set of staging points can be revealed from the geotagging (using the device GPS) and time/date stamping of photos and social media posted on the Internet and recorded in their associated metadata.

As these examples demonstrate, those companies and agencies who run these technologies possess a vast quantity of highly detailed spatial behaviour data from which lots of other insights can be inferred (such as mode of travel, activity and lifestyle). Moreover, these data can be accessed by the police and security forces through warrants or more surreptitiously, and can be shared with third party partners for commercial or governance purposes. Data scientists within, and sometime outside, the institution/corporation generating the data are using analytics to

extract insights and value. The consequence is that individuals are no longer lost in the crowd, but rather they are being tracked and traced at different scales of spatial and temporal resolution, and are increasingly becoming open to geo-targeted profiling and social sorting.

(ii) Inferencing and predictive privacy harms

Predictive modelling using urban big data can generate inferences about an individual that are not directly encoded in a database but constitute what many would consider to be PII and which produce 'predictive privacy harms' [6,51]. For example, tracking data that reveal a person regularly frequents gay bars, leading to the inference that the person is likely to be gay, would be considered by many as personal and sensitive data. If any inference of sexual orientation produced by a predictive model was shared, for example through advertising sent to the family home or via social media on a shared computer, then it could cause personal harm. Yet, as no data about sexuality has been directly collected, any entity making such inferences has 'no obligation under current privacy regimes to give notice to, or gather consent from its customers in the same way that direct collection protocols require' [6, p. 98]. 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 [50,52]. Likewise, the volunteered information of a few people on social media can unlock the same undisclosed information about the many through social network analysis and pattern recognition, creating what Barocas & Nissenbaum [51, p. 61] term the 'the tyranny of the minority'. It has been calculated that knowing the sexual orientation of just 20% of social media users will enable the orientation of all other users to be inferred with a high degree of accuracy [53]. Such inferences can generate inaccurate characterization that then stick to and precede an individual. This is a particular issue in predictive policing and anticipatory governance, where the profiling of both people and places can reinforce or create stigma and harm, particularly when the underlying data or models are poor.

(iii) Anonymization and re-identification

One of the key strategies for ensuring individual privacy is anonymization, either through the use of pseudonyms, aggregation or other strategies. The generation of big data and new computational techniques, however, can make the re-identification of data relatively straightforward in many cases. Pseudonyms, in particular, simply mean that a unique tag is used to identify a person in place of a name. As such, the tag is anonymous in so far that a code is used to identify an individual. However, the code is persistent and distinguishable from others and recognizable on an on-going basis, meaning it can be tracked over time and space and used to create detailed individual profiles [51]. As such, it is no different from other persistent pseudonym identifiers, such as social security numbers, and in effect constitutes PII [54]. The term 'anonymous identifier', as used by some companies (e.g. Google [55]), is thus somewhat of an oxymoron, especially when the identifier is directly linked to an account with known personal details. Pseudonyms 'enable holders of large datasets to act on individuals, under the cover of anonymity, in precisely the ways anonymity has long promised to defend against' and they place no inherent limits on an institution's ability to track and trace the same person in subsequent encounters [51, p. 55]. Further, inference and the linking of a pseudonym to other accounts and transactions means it can potentially be re-identified. Indeed, it is clear that it is possible to reverse engineer anonymization strategies by combing and combining datasets [56,57] unless the data are fully de-identified. De-identification requires both direct identifiers and quasi-identifiers (those highly correlated with unique identifiers) to be carefully removed [59].

(iv) Obfuscation and reduced control

The emerging big data landscape is complex and fragmented. Various smart city technologies are composed of multiple interacting systems run by a number of corporate and state actors

[51,54,60]. For example, the app ecosystem (including app developers, app owners, app stores, operating systems, mobile carriers, devices) is conjoined to the data source ecosystem (e.g. an API of real-time bus data), which similarly consists of a range of hardware, software and organizations. Data are thus passed between synergistic and interoperable 'devices, platforms, services, applications and analytics engines' [50] and shared with third parties. Moreover, across this maze-like assemblage they can be 'leaked, intercepted, transmitted, disclosed, dis/assembled across data streams, and repurposed' in ways that are difficult to track and untangle [50]. The result is that it can be very difficult to know precisely the life of data and how they are used and transformed into new derived data [59]. Nor is it easy to understand the tangled set of roles (as data processors and controllers) and obligations between actors and where responsibilities and liabilities reside [51]. Opacity undermines the fair information practice principles at the heart of privacy regulation in a number of respects: making it difficult for individuals to seek access to verify, query, correct or delete data, or to even know who to ask; to know how data collected about them is used; to assess how fair any actions taken upon the data are; and to hold data controllers to account [5,51,59].

(v) Notice and consent is an empty exercise or is absent

Notice and consent—considered the cornerstone of data and privacy protection—are significantly weakened within smart city technologies and in data/urban science becoming an empty exercise or being entirely absent. Individuals interact with a number of smart city technologies on a daily basis, each of which is generating data about them. Given the volume and diversity of these interactions, it is simply too onerous for individuals to police their privacy across dozens of entities, to weigh up the costs and benefits of agreeing to terms and conditions without knowing how the data might be used now and in the future, and to assess the cumulative and holistic effects of their data being merged with other datasets [60]. Even if someone wanted to proactively manage their data privacy across all these systems and apps, they would be faced with long, complex legal documents that in practice are non-negotiable—one either consents or is denied the service [60,61]. Consent thus often consists of individuals unwittingly signing away rights without realizing the extent or consequences of their actions [62].

In other cases, notice and consent are absent, either unimplemented or difficult to achieve in practice. Between a quarter and a third of all smartphone apps lack a privacy policy and do not seek consent [63]. Notice and consent for downstream activities such as data mining, analysis and repurposing are often covered by catch-all disclaimers, along with the right to unilaterally change terms and conditions without notice, effectively disenfranchising individuals of choice, control and the accountability of service providers. In the case of some smart city technologies, there is little mechanism to seek notice and consent, but also little choice in being surveilled. For example, CCTV, ANPR and MAC address tracking all take place with no attempt at consent and often with little notification. Moreover, there is no ability to opt out [64] other than to avoid the area, which is unreasonable and unrealistic. As such, there is no sense in which a person can selectively reveal themselves; instead they must always reveal themselves. Moreover, if a person is unaware that data about them are being generated, then it is all but impossible to discover and query the purposes to which those data are being put [54,61].

In many cases, those data are being put to work in academic research and in urban science work for which they were not intended. Generally, these studies circumvent notice and consent issues, as well as institutional research boards ethics procedures, by anonymizing/aggregating the data. Nonetheless, the research being undertaken can have effects on those who are unwittingly participating by feeding back into services. This is especially the case in data science practiced within companies and state agencies providing a service. In other cases, studies can ignore ethical procedures altogether arguing that data in the public domain (e.g. social media data or dating site profiles) are open to carte blanche analysis [65] or that they are entitled to experiment on their own systems without user consent [66].

(b) Data use, sharing and repurposing

One of the key features of the data revolution is the wholesale erosion of data minimization principles; that is, the undermining of purpose specification and use limitation principles that mean that data should only be generated to perform a particular task, are only retained as long as they are needed for that task, and are only used to perform a particular task [61]. These principles are largely antithetical to the rationale of big data and the functioning of data markets, which seek to generate and hoard large volumes of data to extract additional value [67]. The solution pursued by many companies is to repackage data by de-identifying them (using pseudonyms or aggregation) or creating derived data, with only the original dataset being subjected to data minimization. The repackaged data can then be sold on and repurposed in a plethora of ways that have little to do with the original reason for data generation and without the need to give notice or consent to those that the data concerns [68].

Such data practices are now common, enabling the rapid growth of data brokers which capture, gather together and repackage data into privately held data infrastructures for rent (for one time use or use under licensing conditions) or re-sale, along with data analysis and profiles [1,69]. Trading data and data services is a multi-billion dollar industry consisting of a diverse ecosystem of different types of data brokers ranging from very large consolidators to a range of specialist companies focused on particular markets or services. In 2014, Angwin [70] identified 212 data brokers operating in the USA that consolidated and traded data about people, only 92 of which allowed opt-outs, and 58 companies that were in the mobile location tracking business, only 11 of which offered opt-outs. Data derived from smart city technologies and associated apps circulate within these data markets.

The data and services these companies offer are used to perform a wide variety of tasks for which the data were never intended, including to predictively profile, socially sort, behaviourally nudge, and regulate, control and govern individuals and the various systems and infrastructures with which they interact [1]. Smart city technologies, the data they generate, and the analytics applied to them thus have significant direct and indirect impact on people's everyday lives. These impacts can be both positive and negative, but in both cases raise numerous questions about privacy and privacy harms. For example, a key product of data brokers are predictive profiles of individuals as to their likely tastes and what goods and services they are likely to buy, or their likely value or worth to a business, or their credit risk and how likely they are to pay a certain price or be able to meet repayments. These profiles can be used to socially sort and redline populations, selecting out certain categories to receive a preferential status and marginalizing and excluding others. Or in the case of urban science to socially sort places to receive certain policy interventions or marketing as practised by the geodemographics industry [71]. This has led to concerns that a form of 'data determinism' is being deployed in which individuals are not simply profiled and judged on the basis of what they have done, but on a prediction of what they might do in the future [72].

Data determinism is most clearly expressed in forms of anticipatory governance, such as that used in predictive policing, where predictive analytics are used to assess likely future behaviours 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 produces both general area profiling to identify hotspots and guide patrols, and more specific profiling that identifies individuals within those hotspots [73]. 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 [73]. In such cases, a person's data shadow does more than follow them; it precedes them.

In all these cases, few of those whose data have fed into creating predictive profiles imagined that their data were going to be repurposed to social sort or regulate or control them, or nudge

them towards certain behaviours. As such, data repurposing can break what is considered compatible forms of data re-use and the reasonable expectations of data subjects [54,61].

4. Recasting smart cities and urban science

There are clearly a number of ethical issues that arise from the creation and deployment of smart city technologies and accompanying urban science and informatics. This has led to a number of critiques concerning the underlying concepts, ethos and practices of smart urbanism [4,9,23,28]. One response to these critiques is to call for a fundamentally different approach to urban development and the practice of other forms of urban studies rather than urban science. Another is to argue that smart cities and urban science need to be re-imagined and re-cast. Rather than throw the baby out with the bath water, it needs to be recognized that smart city technologies do provide many benefits to city managers and citizens. Technologies such as intelligent transport systems do make traffic flow more efficiently around a city and smart phone apps do provide useful services to their users. Similarly, urban science and informatics do provide novel and useful insights into cities, their citizens and systems. This re-imaging and re-casting needs to proceed along three dimensions.

First, there needs to be a re-orientation in how the city is conceived. Rather than being cast as bounded, knowable and manageable systems that can be steered and controlled in mechanical, linear ways, cities need to be framed as fluid, open, complex, multi-level, contingent and relational systems that are full of culture, politics, competing interests and wicked problems and often unfold in unpredictable ways. Reducing this complexity into models and then using the outcomes to drive urban management produces a reductionist and limiting understanding of cities and overly technocratic forms of governance. Rather these models need to be complemented with other forms of knowledge such as phronesis and metis. In other words, city analytics and its instrumental rationality should not be allowed to simply trump reason and experience, or other sources of information and insight such as those based on 'small data' studies, in shaping and driving urban governance. Instead, they should be used contextually and in conjunction with each other.

Second, there needs to be a re-casting of the epistemology of urban science. This re-casting involves recognizing that the realist assumptions, which posit urban science can reveal essential truths about the city, are flawed. Urban science does not, and cannot, provide objective, neutral, God's eye views of the city. Instead, it produces a particular view through a specific lens. On the one hand, the data used do not exist independently of the ideas, instruments, practices, contexts, knowledge and systems used to generate and process them [74]. In other words, data are never raw, but always already cooked [75]. On the other hand, databases and data analytics are similarly not neutral, technical means of assembling and making sense of data but rather are socio-technical in nature, shaped by philosophical ideas and technical means. As such, urban science needs to openly acknowledge its contingencies, shortcomings and inherent politics and to recognize that it does not reflect the world as it actually is, but rather actively frames and produces the world [8]. This is not to say that the fundamental approach of analytics, modelling and simulation is radically altered, but rather that how these approaches work in messy practice is detailed and grand claims as to their veracity or validity is tempered. This would include detailing how ethical issues were considered and the research design altered appropriately.

Third, the ethical dimensions of smart city technologies and urban science need to be much more thoroughly mapped out and addressed. While some might argue that new ethical frameworks based on a gift or sharing basis, in which individuals swap their data for a tangible return (usually a service or knowledge, but also including monetary reward), are in operation or offer an alternative underpinning for a big data economy, smart cities and urban science, the present reality is that many smart city technologies capture data without consent or notice with respect to such a 'gifting' and are so pervasive that the gifting is compulsory with no alternatives. Moreover, the benefits of 'sharing' data are most often stacked in favour of those capturing the data, especially when they are monetized or shared with third parties and used against individual

interests. In order for a sharing notion of ethical practice to be enacted, those gifting the data must have full details of what data are being generated, what additional data are being inferred from them, *and* to have shared control and benefit in how all data relating to them are subsequently used. This requires full notice and consent, as well full transparency with respect to the actions of data controllers and processors. Currently, such an ethical model is a long way from being enacted. Therefore, the ethical concerns raised in this paper need to be continued to be addressed from a more traditional privacy rights perspective.

Researchers need to consider the ethical implications of their work with respect to privacy harms, notice and consent, and the uses to which their research is being deployed. Beyond complying with relevant laws and institutional research board requirements, analysts have a duty of care to their fellow citizens not to expose them to harm through their analysis. Admittedly, what constitutes harm is often difficult to define and harms can occur directly or indirectly but nonetheless there is a need to consider how research might be used and to act responsibly. In addition, professional bodies should review their ethical standards in the light of big data and revise accordingly. City managers need to consider the potential pernicious effects of the roll-out of smart city technologies and that notice and consent are all but impossible in many cases and take a pro-active role in brokering privacy and security arrangements on behalf of citizens through its contracting procedures and parameters. Here, all vendors would be compelled to comply with service level agreements concerning the operation of systems, what data are generated and how these can be used and shared, and be subject to privacy impact assessments.

We need to create smart cities and urban science that have a set of ethical principles and values at their heart. The challenge is to acknowledge that there are a number of very real ethical issues and concerns that need to be addressed, and to find and adopt solutions to these that also enable the benefits of smart city technologies to be realized. This is no easy task, but one that needs urgent redress and this paper has sought to map out relevant issues and to suggest a viable path forward.

Competing interests. I declare I have no competing interests.

Funding. The research for this paper was funded by an ERC Advanced Investigator award (ERC-2012-AdG 323636-SOFTCITY) and by the Data Forum of the Department of the Taoiseach, Ireland, for a study entitled: 'Getting Smarter about Smart Cities: Improving Data Privacy and Data Security'.

References

1. Kitchin R. 2014 *The data revolution: big data, open data, data infrastructures and their consequences*. London, UK: Sage.
2. Graham S, Marvin S. 2001 *Splintering urbanism: networked infrastructures, technological mobilities and the urban condition*. New York, NY: Routledge.
3. Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, Wachowicz M, Ouzounis G, Portugali Y. 2012 Smart cities of the future. *Eur. Phys. J. Special Topics* **214**, 481–518. (doi:10.1140/epjst/e2012-01703-3)
4. Kitchin R. 2014 The real-time city? Big data and smart urbanism. *GeoJournal* **79**, 1–14. (doi:10.1007/s10708-013-9516-8)
5. Strandberg KL. 2014 Monitoring, datafication and consent: legal approaches to privacy in the big data context. In *Privacy, big data and the public good* (eds J Lane, V Stodden, S Bender, H Nissenbaum), pp. 5–43. Cambridge, UK: Cambridge University Press.
6. Crawford K, Schultz J. 2014 Big data and due process: toward a framework to redress predictive privacy harms. *Boston College Law Rev.* **55**, 93–128.
7. Townsend A. 2013 *Smart cities: big data, civic hackers, and the quest for a new Utopia*. New York, NY: W.W. Norton & Co.
8. Kitchin R, Lauriault TP, McArdle G. 2015 Knowing and governing cities through urban indicators, city benchmarking & real-time dashboards. *Reg. Stud. Reg. Sci.* **2**, 1–28. (doi:10.1080/21681376.2014.983149)
9. Marvin S, Luque-Ayala A, McFarlane C (eds). 2016 *Smart urbanism: Utopian vision or false dawn?* London, UK: Routledge.

10. Centro De Operacoes Prefeitura Do Rio. See http://centrodeoperacoes.rio/institucional
11. Singer N. 2012 Mission control, built for cities: IBM takes 'smarter cities' concept to Rio de Janeiro. *New York Times*, 3 March 2012. See http://www.nytimes.com/2012/03/04/business/ibm-takes-smarter-cities-concept-to-rio-de-janeiro.html (accessed 9 May 2013).
12. Foth M (ed.) 2009 *Handbook of research on urban informatics: the practice and promise of the real-time city*. Hershey, PA: IGI Global.
13. Batty M. 2013 *The new science of cities*. Cambridge, MA: MIT Press.
14. Ratti C, Offenhuber D. 2014 *Decoding the city: how big data can change urbanism*. Basel, Switzerland: Birkhauser Verlag AG.
15. Lazer D *et al.* 2009 Computational social science. *Science* **323**, 721–733. (doi:10.1126/science.1167742)
16. Miller HJ. 2010 The data avalanche is here. Shouldn't we be digging? *J. Reg. Sci.* **50**, 181–201. (doi:10.1111/j.1467-9787.2009.00641.x)
17. Bunge W. 1962 *Theoretical geography*. Lund Studies in Geography Series C: General and Mathematical Geography. Lund, Sweden: Gleerup.
18. Haggett P. 1966 *Locational analysis in human geography*. New York, NY: St Martin's Press.
19. Tobler WR. 1959 Automation and cartography. *Geogr. Rev.* **XLIX**, 526–534. (doi:10.2307/212211)
20. Tomlinson RF. 1968 A geographic information system for regional planning. In *Land evaluation* (ed. GA Stewart), pp. 200–210. Melbourne, Australia: Macmillan.
21. Forrester JW. 1969 *Urban dynamics*. Encino, CA: Pegasus Communications.
22. Desrosieres A. 1998 *The politics of large numbers: a history of statistical reasoning*. Cambridge, MA: Harvard University Press.
23. Mattern S. 2013 Methodolatry and the art of measure: the new wave of urban data science. *Design Observer: Places*, 5 November 2013. See http://designobserver.com/places/feature/0/38174/ (accessed 15 November 2013).
24. Morozov E. 2013 *To save everything, click here: technology, solutionism, and the urge to fix problems that don't exist*. New York, NY: Allen Lane.
25. Buttimer A. 1976 Grasping the dynamism of lifeworld. *Ann. Assoc. Am. Geogr.* **66**, 277–292. (doi:10.1111/j.1467-8306.1976.tb01090.x)
26. Flood J. 2011 *The fires: how a computer formula, big ideas, and the best of intentions burned down New York city—and determined the future of cities*. New York, NY: Riverhead.
27. Harvey D. 1973 *Social justice and the city*. London, UK: Edward Arnold.
28. Greenfield A. 2013 *Against the smart city*. New York, NY: Do Publications.
29. Parsons W. 2004 Not just steering but weaving: relevant knowledge and the craft of building policy capacity and coherence. *Austr. J. Public Admin.* **63**, 43–57. (doi:10.1111/j.1467-8500.2004.00358.x)
30. Bettencourt LMA, Lobo J, Helbing D, Kühnert C, West GB. 2007 Growth, innovation, scaling, and the pace of life in cities. *Proc. Natl Acad. Sci. USA* **104**, 7301–7306. (doi:10.1073/pnas.0610172104)
31. Pentland A. 2014 *Social physics: how good ideas spread—the lessons from a new science*. New York, NY: Penguin.
32. Anderson C. 2008 The end of theory: the data deluge makes the scientific method obsolete. *Wired*, 23 June 2008. See http://www.wired.com/science/discoveries/magazine/16-07/pb_theo-ry (accessed 12 October 2012).
33. Kelling S, Hochachka W, Fink D, Riedewald M, Caruana R, Ballard G, Hooker G. 2009 Data-intensive science: a new paradigm for biodiversity studies. *BioScience* **59**, 613–620. (doi:10.1525/bio.2009.59.7.12)
34. Elwood S, Leszczynski A. 2011 Privacy reconsidered: new representations, data practices, and the geoweb. *Geoforum* **42**, 6–15. (doi:10.1016/j.geoforum.2010.08.003)
35. Martínez-Ballesté A, Pérez-Martínez PA, Solanas A. 2013 The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Commun. Mag.* **51**, 136–141. (doi:10.1109/MCOM.2013.6525606)
36. Santucci G. 2013 Privacy in the digital economy: requiem or renaissance? *Privacy Surgeon*. See http://www.privacysurgeon.org/blog/wp-content/uploads/2013/09/Privacy-in-the-Digital-Economy-final.pdf (accessed 12 November 2015).
37. Solove DJ. 2006 A taxonomy of privacy. *Univ. Penn. Law Rev.* **154**, 477–560. (doi:10.2307/40041279)

38. Dodge M, Kitchin R. 2005 Codes of life: identification codes and the machine-readable world. *Env. Plan. D Society Space* **23**, 851–881. (doi:10.1068/d378t)
39. Clarke R. 1988 Information technology and dataveillance. *Commun. ACM* **31**, 498–512. (doi:10.1145/42411.42413)
40. Raley R. 2013 Dataveillance and countervailance. In *'Raw data' is an oxymoron* (ed. L Gitelman), pp. 121–146. Cambridge, MA: MIT Press.
41. Crampton J. 2003 Cartographic rationality and the politics of geosurveillance and security. *Cart. Geo. Info. Sci.* **30**, 135–148. (doi:10.1559/152304003100011108)
42. Graham S. 2011 *Cities under siege: the new military urbanism*. London, UK: Verso.
43. Gardham M. 2015 Controversial face recognition software is being used by Police Scotland, the force confirms. *Herald Scotland*, 26 May 2011. See http://www.heraldscotland.com/news/13215304.Controversial_face_recognition_software_is_being_used_by_Police_Scotland__the_force_confirms/ (accessed 13 November 2015).
44. Wellman T. 2015 Facial recognition software moves from overseas wars to local police. *New York Times*, 12 August 2015. See http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html (accessed 13 November 2015).
45. Weaver M. 2015. Warning of backlash over car number plate camera network. *The Guardian*, 27 November 2015. See http://www.theguardian.com/uk-news/2015/nov/26/warning-of-outcry-over-car-numberplate-camera-network (accessed 7 December 2015)..
46. Vincent J. 2014 London's bins are tracking your smartphone. *The Independent*, 10 June 2014. See http://www.independent.co.uk/life-style/gadgets-and-tech/news/updated-londons-bins-are-tracking-your-smartphone-8754924.html (accessed 13 November 2015).
47. Henry A. 2013 How retail stores track you using your smartphone (and how to stop it). *Lifehacker*, 19 July 2013. See http://lifehacker.com/how-retail-stores-track-you-using-your-smartphone-and-827512308 (accessed 15 November 2015).
48. Goodman M. 2015 *Future crimes: a journey to the dark side of technology—and how to survive it*. New York, NY: Bantam Press.
49. What they know—mobile. *Wall Street Journal*. See https://blogs.wsj.com/wtk-mobile/.
50. Leszczynski A. In press. Geoprivacy. In *Understanding spatial media* (eds R Kitchin, T Lauriault, M Wilson). London, UK: Sage.
51. Baracos S, Nissenbaum H. 2014 Big data's end run around anonymity and consent. In *Privacy, big data and the public good* (eds J Lane, V Stodden, S Bender, H Nissenbaum), pp. 44–75. Cambridge, UK: Cambridge University Press.
52. Soltani A, Gellman B. 2013 New documents show how the NSA infers relationships based on mobile location data. *The Washington Post*, 10 December 2013. See http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/ (accessed 14 October 2015).
53. Mislove A, Viswanath B, Gummadi KP, Druschel P. 2010 You are who you know: inferring user profiles in online social networks. In *Proc. 3rd ACM Int. Conf. on Web Search and Data Mining*, pp. 251–260. New York, NY: ACM. (doi:10.1145/1718487.1718519)
54. Article 29 Data Protection Working Party. 2014 Opinion 8/2014 on the recent developments on the internet of things. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (accessed 4 November 2015).
55. Google. Privacy and terms. See https://www.google.com/policies/privacy/key-terms/.
56. Narayanan A, Shmatikov V. 2010 Privacy and security: myths and fallacies of 'personally identifiable information'. *Commun. ACM* **53**, 24–26. (doi:10.1145/1743546.1743558)
57. de Montjoye YA, Hidalgo CA, Verleysen M, Blondel VD. 2013 Unique in the crowd: the privacy bounds of human mobility. *Sci. Rep.* **3**, 1376. (doi:10.1038/srep01376)
58. Cavoukian A, Castro D. 2014 *Big data and innovation, setting the record straight: de-identification does work*. Ontario, Canada: Information and Privacy Commissioner. See http://www2.itif.org/2014-big-data-deidentification.pdf (accessed 20 November 2015).
59. Fuster GG, Scherrer A. 2015 Big Data and smart devices and their impact on privacy. Committee on Civil Liberties, Justice and Home Affairs (LIBE), Directorate-General for Internal Policies, European Parliament. See http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf (accessed 4 November 2015).

60. Solove D. 2013 Privacy management and the consent dilemma. *Harvard Law Rev.* **126**, 1880–1903.
61. European Data Protection Supervisor. 2014 Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the digital economy. See http://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf (accessed 4 November 2015).
62. Rubinstein IS. 2013 Big data: the end of privacy or a new beginning? *Int. Data Privacy Law* **3**, 74–87. (doi:10.1093/idpl/ips036)
63. Zang J, Dummit K, Graves J, Lisker P, Sweeney L. 2015 Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*, 30 October 2015. See http://jots.pub/a/2015103001/ (accessed 9 November 2015).
64. Crump C, Harwood M. 2014 Invasion of the data snatchers: big data and the internet of things means the surveillance of everything. *ACLU*, 25 March 2014. See http://www.aclu.org/blog/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything (accessed 22 November 2015).
65. Resnick B. 2016 Researchers just released profile data on 70,000 OkCupid users without permission. *Vox*, 12 May 2016. See http://www.vox.com/2016/5/12/11666116/70000-okcupid-users-data-release (accessed 13 May 2016).
66. Booth R. 2014 Facebook reveals news feed experiment to control emotions. *The Guardian*, 30 June 2014. See https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds (accessed 13 May 2016).
67. Tene O, Polonetsky J. 2012 Big data for all: privacy and user control in the age of analytics. *Social Sciences Research Network*, 20 September 2012. See http://ssrn.com/abstract=2149364 (accessed 15 July 2013).
68. Solove DJ. 2007 'I've got nothing to hide' and other misunderstandings of privacy. *Social Sciences Research Network*, 12 July 2007. See http://ssrn.com/abstract=998565 (accessed 16 July 2013).
69. CIPPIC. 2006 On the data trail: how detailed information about you gets into the hands of organizations with whom you have no relationship. A report on the Canadian data brokerage industry. Ottawa, Canada: Canadian Internet Policy and Public Interest Clinic. See http://www.cippic.ca/uploads/May1-06/DatabrokerReport.pdf (accessed 17 January 2014).
70. Angwin J. 2014 *Dragnet nation*. New York, NY: St Martin's Press.
71. Graham S. 2005 Software-sorted geographies. *Progr. Hum. Geogr.* **29**, 562–580. (doi:10.1191/0309132505ph568oa)
72. Rameriz E. 2013 The privacy challenges of big data: a view from the lifeguard's chair. Technology Policy Institute Aspen Forum, 19 August 2013. See http://ftc.gov/speeches/ramirez/130819bigdataaspen.pdf (accessed 11 October 2013).
73. Stroud M. 2014 The minority report: Chicago's new police computer predicts crimes, but is it racist? *The Verge*, 19 February 2014. See http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist (accessed 30 November 2015).
74. Ribes D, Jackson SJ. 2013 Data bite man: the work of sustaining long-term study. In *'Raw data' is an oxymoron* (ed. L Gitelman), pp. 147–166. Cambridge, MA: MIT Press.
75. Bowker G. 2005 *Memory practices in the sciences*. Cambridge, MA: MIT Press.