People watching: Abstractions and orthodoxies of monitoring

Victoria Wang, John V. Tucker

PII: S0160-791X(22)00319-0

DOI: https://doi.org/10.1016/j.techsoc.2022.102178

Reference: TIS 102178

To appear in: *Technology in Society*

Received Date: 16 July 2022

Revised Date: 18 November 2022

Accepted Date: 19 November 2022

Please cite this article as: Wang V, Tucker JV, People watching: Abstractions and orthodoxies of monitoring, *Technology in Society* (2022), doi: https://doi.org/10.1016/j.techsoc.2022.102178.

People watching:
abstractions and orthodoxies of monitoring

1. Victoria Wang

Corresponding Author
victoria.wang@port.ac.uk

School of Criminology and Criminal Justice, St George's Building, 141 High Street, Portsmouth, PO1 2HY, UK

2. John V. Tucker

Co-author
j.v.tucker@swansea.ac.uk

Department of Computer Science, Computational Foundry, Swansea University, Swansea, SA1 8EN, UK

People watching:
abstractions and orthodoxies of monitoring

1. Victoria Wang

Corresponding Author
victoria.wang@port.ac.uk

School of Criminology and Criminal Justice, St George's Building, 141 High Street, Portsmouth, PO1 2HY, UK

2. John V. Tucker

Co-author
j.v.tucker@swansea.ac.uk

Department of Computer Science, Computational Foundry, Swansea University, Swansea, SA1 8EN, UK

People watching:
abstractions and orthodoxies of monitoring

Abstract

Our society has an insatiable appetite for data. Much of the data is collected to monitor the activities of people, e.g., for discovering the purchasing behaviour of customers, observing the users of apps, managing the performance of personnel, and conforming to regulations and laws, etc. Although monitoring practices are ubiquitous, monitoring as a general concept has received little analytical attention. We explore: (i) the nature of monitoring facilitated by software; (ii) the structure of monitoring processes; and (iii) the classification of monitoring systems. We propose an abstract definition of monitoring as a theoretical tool to analyse, document, and compare disparate monitoring applications. For us, monitoring is simply the systematic collection of data about the behaviour of people and objects. We then extend this concept with mechanisms for detecting events that require interventions and changes in behaviour, and describe five types of monitoring.

We argue for the development of a general theory of monitoring.

Keywords: monitoring, interventions, software, data, surveillance

1. Introduction

Developments in data collection, computation, and communication are making possible a comprehensive monitoring of everyday life – as individuals, or as members of social and economic groups, or of organisations and companies. Certainly, we have become accustomed to being monitored, much of which is *supposed* to be good for us. In both the physical and virtual world, the general activities and professional performance of people and organisations are being captured by various monitoring technologies and reduced to digital data. These monitoring technologies have helped create large commercial sectors serving security, retailing, logistics, accreditation and regulation, and social interaction.

Digital data can be collected, processed, stored, sorted, searched, shared, combined, altered, stolen and destroyed, all relatively easily, remotely and at scale. Data has been re-invented as a new multidisciplinary field of research, symbolised by the coinage of the term 'big data' by Douglas Laney [1]. Monitoring has enabled the development of big data and stimulated a hunger for more data and more monitoring. These effects have become prominent in the past two decades, in terms of the volume of data created, as well as its diversity and commercial value, e.g., [2]. Indeed, big data is central to a new economic logic, named surveillance capitalism [3, 4, 5]. It is based on the trading of access to digital data generated by individuals' daily routines in order to directly influence and modify their behaviour for profit [6]. These changes are made possible by the theories and methods in computer science coming to practical maturity (e.g., in databases, machine learning, visual computing).

Our curiosity about monitoring began with our observation of its presence in our everyday lives and in its implicit role in debates in surveillance studies – a multidisciplinary subject studying both theories and empirical practices of surveillance in society. Surveillance studies is a blanket term encompassing a wide range of contexts and practices of a social, economic, legal and political kind. It also depends upon classic philosophical and sociological abstractions, such as trust, privacy, identity, and security. To these abstractions we propose to add monitoring.

In this paper, we report on our initial theoretical exploration of the concept of monitoring. We aim to establish it as an independent subject for investigation and discussion. Thus, our two research questions are:

(i) Can monitoring be abstracted from its countless manifestations and practices, and subsequently be constituted as an independent topic of study?

(ii) What basic concepts are involved in monitoring, and can they be used to build a general theory to study monitoring and its effects?

We begin our exploration by discussing some of the practices that motivate and shape our study of monitoring. We then propose abstract definitions to make precise questions and frame answers about any monitoring process:

1. What are the objects or people that are monitored?
2. What are the behaviours of the objects or people to be examined, and how are they represented as digital data?
3. What properties of the behavioural data are to be observed and recorded?
4. What is done with the data in these records?

The purpose of monitoring is to collect and store data. Records of observations can be checked for points of interest, or for what is unusual, and enable historical search and investigation if the need arises. Typically, monitoring is used

- to see that certain things do or do not happen – *conformance monitoring* – as in management and criminal justice; and
- to gain insight and information – *discovery monitoring* – as in the sciences and retail.

There are centuries old examples of both types of monitoring that do not bring surveillance to mind: financial accounting is based on conformance monitoring; and astronomy, meteorology, and natural history are based on discovery monitoring.

In our conceptual framework, we make a distinction between the collection of data and any actual use that is made of it. Thus, we propose two definitions to theorise monitoring:

i) a *passive* one that only observes and records, and

ii) an *active* one with interventions that may notify or change behaviour.

Our abstract definitions are intended to establish a conception of monitoring for digital data that can deployed in theory and practice, e.g., through ontologies to help discover and document answers to the previous four questions in whatever domains they are raised.

Our exploration of monitoring as an independent subject area builds on established research in surveillance studies. According to David Lyon, surveillance refers to “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or detection” [7: 14]. It has three abstract purposes: (i) control, (ii) social sorting, and (iii) mutual monitoring [8].

No matter the purpose, the monitoring of everyday life rests at the heart of contemporary surveillance studies and practices. In fact, this is stated in the title of Lyon’s seminal book – *Surveillance society: Monitoring everyday life* [9]. Now, as everyday life is enabled and sustained by software and data, we should take a deep interest in computer systems. Indeed, surveillance practices depend on digital technologies that enable the monitoring of everyday life. As monitoring is record keeping, it is fundamental to surveillance.

Monitoring looks at and measures the ‘health’ of all forms of computer systems; it generates logs that are designed to reveal what and when events took place, and who or what caused them. And there are many kinds of logs lying beneath the surface of the software that brings the world’s users together. Of course, monitoring is not only about infrastructure, devices and data collection. Studying monitoring’s influence in human affairs overlaps – some will say needlessly trespasses on – surveillance studies. For those interested in a particular domain it can be hard to see a value in studying monitoring *per se* and the technologies of automatic record keeping; but for those interested in general theories of society abstract ideas about monitoring ought to be most welcome.

Our exploration focuses on three aspects: (i) the nature of monitoring relating to software; (ii) the abstract structure of monitoring processes; and (iii) typologies of monitoring processes according to purpose or actual use. These are discussed in the following sections of this paper, respectively. First, to provide technical arguments for an independent theory, in Section 2, we provide a simple initial definition of monitoring, situate our arguments on monitoring by computer systems, and by reflecting on the role of monitoring in ‘big data’ and surveillance. Surveillance has large, diverse and well-established literatures, in which the effects of monitoring play a role but monitoring itself is rarely centre stage.

Secondly, in Section 3, we offer a rigorous abstract definition of monitoring as a process that observes people or objects by choosing data to measure or represent their behaviour, testing the data for certain properties, and lastly recording the degree the behaviour data exhibits the properties. The definition is designed to apply to a diverse collection of monitoring situations; we illustrate the definition with simple examples of monitoring in management, retail, and criminal justice. Thirdly, in Section 4, we develop a second abstract definition of monitoring in which information recorded by a monitoring system can initiate actions that we call interventions. It is the interventions that specify or reveal what the monitoring data is actually used for. We illustrate the definition of monitoring with interventions by discussing five overlapping abstract types, namely: (i) access control systems; (ii) permission systems; (iii) penalty systems; (iv) incentive systems; and (v) recommendation systems. In Section 5, we conclude and, encouraged by our initial findings, we call for further investigations to help establish monitoring as a subject with many specialisations.

2. Monitoring – Defined and Situated

After elaborating on our approach to making a theory of monitoring, we address its relationship with data science and surveillance studies, and comment on old and new monitoring processes.

2.1 Our approach

Let us begin with proposing a simple idea of the process of monitoring.

Initial definition. A *monitoring technology* is a means of observing and recording properties of the behaviour of an object or a person in a context. A monitoring technology generates records. In fact, the context is best defined by the properties observed by the technology.

Given the diversity of monitoring situations, applying such an informal definition naturally leads to other terminologies that are better suited to specific contexts and domains. A context may be better served by replacing our term *observing* by measuring, logging, recognising, sensing, or detecting; our term *property* might be replaced by attribute, feature, symptom, or event; and the term *behaviour* might be replaced by state, mode, trace, history, trajectory, trend, and so on. Our approach to theorising has four features.

First, it seeks abstract concepts, frameworks and formal tools that have considerable generality, and can be applied to cases diverse in nature and separated in time.

Second, it is concerned *only with data*. It is not directly concerned with the people and objects themselves, but it is concerned with *data about* their behaviour and *data about* their identity. This data is *digital* which nowadays includes numbers, texts, sounds, images, videos, haptics etc.

Third, in replacing our informal definition, our abstract definitions attempt to identify and make precise the essential components of monitoring. This brings benefits: (a) in any situation, they are guides to identify and examine what processes monitor what behaviour; and (b) they allow us to further abstract, model and reason using algebra and logic and to relate formally to the monitoring activities of apps and platforms.

Fourth, we view the acquisition of data as independent of its subsequent use. By focussing on sources of data, it also helps detect commonalities and distinctions relevant to real-world practices in diverse domains. The commonalities of data gathering are simpler to uncover and understand than the diversities of the use of monitoring data. This separation of concerns enables us to identify intentional versus unintentional uses of monitoring data.

This approach seeks conceptual structures and ontologies that may be customised to guide empirical investigations, such as:

- *Provenance of data sets*: Many data sets of value and practical use are created from initial data by all sorts of computations involving combinations and linkages with other data sets. Monitoring processes are one source of initial data; their provenance and characteristics need to be known to judge if the constructed data set is 'fit-for-purpose', practically or ethically.
- *System guarantees*: To better understand and certify (say) privacy properties for a software product or service, a provider might require a rigorous analysis of the data it acquires, creates, and destroys in its deployment and practical use. The number and complexity of software and data components need mathematical tools to make such evaluations.
- *Business intelligence and efficiency*: An internal audit of monitoring practices might reveal what data is available to an organisation, if and when the data is used, and what new value (or risk) might it offer (or reveal). In our experience, monitoring can be casually motivated, naively specified, and crudely expressed in metrics.

- *Regulation by law or good practice:* To satisfy governments, regulators and accrediting bodies, organisations will need to authenticate their operations with analytical reports based on monitoring records (which may be subject to inspection).

2.2 Big data and monitoring

Contemporary data science, nicknamed 'big data', applies algorithmic methods to construct and explore data sets with diverse origins and purposes. Seemingly unrelated data sets can be combined with dramatic effects, e.g., on privacy, something that complicates government open data initiatives [10, 11]. However, technically, data sets have many common properties. It is more than 20 years since Laney's [1] handy technical description of data sets by volume, velocity, and variety ('3Vs') and many more characteristics have been noted, e.g., [12].[1] A survey can be found in [13].

How much of this big data has monitoring as its source? We think that monitoring is a primary source of data about the world and so expect it to be a primary component of big data. This is borne out by studies of the origins of data sets commonly in use and their classification, such as the three high-level types identified in [14], or the 13 subtypes unpacked in [15: 9].[2] In 2015, the United Nations Economic Commission for Europe (UNECE) gave a *Big Data Source Taxonomy* that also identified three main sources of data:

1. *Human-sourced information*: data produced by social media networks; blogs and posted comments; personal documents; pictures; videos; internet searches; text messages; user-generated maps; and emails.
2. *Process-mediated/transaction data*: data produced by public agencies and businesses.
3. *Machine-generated data***:** data produced by fixed sensors; mobile sensors; satellites; logs of computer systems and networks.

[1] To Laney's criteria they add: exhaustivity; resolution; indexicality; relationality; extensionality; and scalability to make nine traits of data sets.

[2] These are: (i) directed data; (ii) automated data; (iii) automated surveillance; (iv) digital devices; (v) sensed data; (vi) scan data; (vii) interaction data; (viii) volunteered data; (ix) transactions; (x) social media; (xi) sousveillance; (xii) crowdsourcing; and (xiii) citizen science.

This UNECE classification, with its 24 subcategories, has settled down and become something of a standard that is commonly used in statistical circles related to government.[3] In cataloguing examples of data sets by types, the answer to the question becomes clear: monitoring is a main source for the raw material of data science, and for its contemporary controversies, some of which morph into surveillance.

Early on, data science was claimed to be establishing a new paradigm of scientific research [16] and changing the study of social, political, and economic life [17, 15]. Data science promises a new general empirical epistemology with new forms of knowledge and predictive tools, underwritten by the authority of measurement. This focusses attention on monitoring, attitudes to quantification and data, and their enhanced role in evidence gathering and decision making. The hold this general empirical paradigm has on organisations and companies increases the need for more monitoring. The paradigm raises some important questions that have been concisely surveyed in [18, 19].

2.3 Surveillance and monitoring

Next, we situate our concept of monitoring in the context of surveillance studies.

In their critical survey, Galič et al. [2] propose surveillance theories could be structured in three chronological/thematic phases:

i) Bentham and Foucault's panoptic structures of power inspired by physical architecture;

ii) Deleuze, Haggerty and Ericson, and Zuboff's networked surveillance relying mainly on digital technologies;

iii) scholarship that conceptualises surveillance through notions, including dataveillance, social sorting, and peer-to-peer surveillance.

Independent of old metaphors and new notions, thanks to the 'datafication' of everyday life, surveillance practices are becoming relevant to every arena of our daily lives.

[3] The 2020 version uses popular names for the three high-level categories, namely: Social Networks, Traditional Business Systems, Internet of Things, respectively: https://statswiki.unece.org/display/bigdata/Classification+of+Types+of+Big+Data

Recall that for us, monitoring highlights infrastructure, made by combining devices and software. Thus, our understanding of monitoring resonates with Deleuze's [20] writing in the early 1990s prior to the prevalence of networked technologies. He focused on open spaces and paid attention to control at a distance through technologies. Drawing on Deleuze's work, Haggerty and Ericson introduced the idea of 'data doubles' in their seminal paper *The surveillant assemblage* [21]. For them, a 'surveillance assemblage' is a 'convergence of discrete surveillance systems', which 'operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows' [11: 606]. 'These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention' [21]. As a result, the panoptic hierarchy of surveillance is levelled: big brother becomes a diaspora of little (and not so little) big brothers [22, 23]; and more individuals and groups are being monitored for new purposes, including deterrence, consumption, entertainment, health promotion, education, governance, accountability, child-care and military success [21, 24].

Particularly, surveillance today is increasingly used in economic contexts, e.g., to motivate, generate and monitor consumption patterns. This use is, nevertheless, not at all new. Karl Marx understood surveillance as both an economic and a political concept in his theory of society [25]. Capturing its contemporary economic aspect, the notion of surveillance capitalism was first used by Bellamy and McChesney [26], and subsequently analysed and made known by Zuboff [27, 5, 6] as 'a wholly new subspecies of capitalism in which profits derive from the unilateral surveillance and modification of human behavior' [6: 1]. Zuboff suggests that surveillance capitalism comprises 'an emergent logic of accumulation' of digital traces, which 'produces its own social relations and with that its conceptions and uses of authority and power' [27: 77]. She further identifies four key features of surveillance capitalism: i) the insatiable appetite for data extraction and analysis; ii) the real-time monitoring of contractual performance along with real-time, technology-enabled enforcement of contract; iii) personalised and customised services; iv) the continual experimentation and intervention into users' lives [6]. Big data and monitoring are the essential features of surveillance capitalism, which is based on data collection, predictive logics and their profitability [2].

Propelled by developments in technologies, new terminologies have emerged to describe new approaches to surveillance. Here are some examples [28, 29]:

- Whilst the term *surveillance* tends to be associated with the powerful watching the less powerful, the term *sousveillance* is often used to mean the less powerful watching the more powerful.
- Whilst the term *panoptic veillance* tends to be associated with the few watching the many, the term *synoptic veillance* is often used to mean the many watching the few.
- *Banoptic surveillance* describes the exclusion of individuals or social groups via surveillance techniques.
- *Participatory veillance* describes the voluntary participation as a subject of veillance.

Most of these new terminologies retain the word *veillance*, which originates in the French word *veiller* – a *neutral* form of watching, which is suggestive of monitoring. In fact, elements of monitoring could be found in almost all current understandings of surveillance. For example, Morgan [30] pointed out that discussions of sousveillance [31] had accelerated among individuals who develop their own approaches and exercise self-monitoring for their own reasons. Subsequently, numerous self-monitoring, tracking and data-gathering technologies have been developed, particularly in the health and wellbeing sector [32] and at workplaces [33]. For another example, in terms of panoptic surveillance, its contemporary interpretation includes the expectation of subjects to better themselves by engaging in self-surveillance, i.e., to monitor and manage their own behaviours in accordance with the social norms in their contexts [34]. For a third example, participatory surveillance is a form of community-based monitoring via a series of intelligence gathering technologies (e.g., 'track and trace' apps) and techniques (e.g., self-reporting) [35], which is particularly dominant in the public health sector (e.g., infection control for Covid-19) [36, 37].

Some new terminologies that reference the technical dimension of surveillance have also emerged. Here are some examples [28, 29]:

- The term *dataveillance/panspermic veillance* means watching that involves the use of digital data technologies rather than human senses alone. In the virtual world, the term *algorithmic veillance* means watching using computer algorithms and digital data.
- The term *uberveillance* means watching from all directions, particularly with the use of tracking devices worn on, or embedded in, the human body.
- The term *social veillance* means watching each other via social media.

- *Liquid surveillance* means watching that is dynamic or fluid, moving restlessly from site to site and using various types of technologies.

These concepts with their particular emphases may shape our perspectives on surveillance. The role of monitoring as we see it is evident in all of them. Our own view of monitoring is closest to dataveillance and algorithmic veillance.

Our abstract descriptions of monitoring build on formal studies of surveillance. In Wang and Tucker [38, 39], an abstract general notion of surveillance system was defined to cover many examples and even allow a mathematical model to be developed that focused on digital identity.[4] These abstract analyses of surveillance led us to think abstractly about monitoring.

2.4 Types of Monitoring Technologies

In this light, surveillance thus becomes a concept that depends on many technologies networked together. Networking involves systems communicating, which introduces the fundamental practical issue of identity: are the systems observing the same entity (person, object, or class of such). Large commercial sectors have been created serving security, retailing and social interaction. Prominent are technologies for monitoring.

To take a timely example, automated face recognition (AFR) for gaining access is becoming common for phones and other gadgets, e.g., vending machines associated with payments via *Alipay* and *WeChat* in China [40]. To the well-established technologies of monitoring by video camera, AFR adds enormous functionality as it offers a solution to problems of identification when needed. Of course, traffic cameras of all kinds have solved identification problems for vehicles through number plate recognition with profound practical consequences for traffic control and general police investigations. AFR promises more profound consequences, perhaps. Together with its technical promise of AFR comes associated ethical and legal debates to do with its application, as well as general privacy challenges [41, 42]. In the UK, for example, the use of face recognition by South Wales Police since 2017 has been a testcase in the courts, e.g., South Wales Police [43, 44] and Court of Appeal [45].

[4] It observed that since surveillance systems are largely digital then mathematical methods that model data, software and hardware can be adapted to analyse surveillance practices.

Keeping pace with computing trends, monitoring has already become a service that can be outsourced (MaaS) to cloud-based service companies with highly specialised knowledge.[5] Organisations with many employees depend on many devices and applications; the performance of these digital tools affects people's productivity and working experience. The performance monitoring of devices and software across a geographically distributed organisation can be outsourced.[6] At least that's how MaaS starts: what gets measured about people's activities and reported to management is open-ended.

As processors, software and data become embedded and networked in the physical world, creating smart urban and domestic environments, monitoring is necessarily ubiquitous and pervasive. Monitoring depends on technologies for collecting data, and it is useful to recall the origins of the phase *internet of things* (IoT): it was coined by Kevin Ashton of Procter & Gamble in 1999 to conceptualise a beautiful solution to a stock control problem for lipsticks in stores. The solution was to use RFID tags in order to expand the gathering of data that can then be processed by monitoring software that would intervene when stocks were low. The general computational problem addressed by Ashton's conception of the IoT is simply *data input at scale* [47: xvi-xviii]. Adding processors expands data gathering and pre-processing.

A most important class of monitoring tool is the non-so humble *computer log* that records the commands and data of software as it executes. Typically, actions are listed in order, classified by relevant tags and timestamped; if mobile, the computational actions can be tagged by location. Logs are designed as a source of information about the functioning of software for its technical performance, business value and user experience. For example, a company ought to be interested in the performance of its webpages. Browsers can collect relevant information. The WC3, the consortium that guide web development, has a specification for browsers to collect data that measures timings; it contains 21 basic measurements, and from these further timing metrics may be computed and statistics generated [48: 69-71]. In addition to computational performance for users, companies can use web analytics, like the widely used

[5] MaaS follows the movement towards 'computing as a service' that outsources software (SaaS), platforms (PaaS), and infrastructure (IaaS).

[6] Compare the monitoring of employees of what are currently called Digitial Employee Experience (DEX) tools [46].

Google Analytics, a service launched by Google in 2005 after acquiring Urchin. Tagging users via their devices, geographically or virtually, is a basic source of machine-generated data.

The intimate relationship between computers, logs and monitoring is abstracted by the concept of *logject* for objects employing software that log their own use [49, 50]. The records can be stored, transmitted and analysed anywhere. The smart phone is an advanced example – it manages itself, is location aware, adapts to the environment, recognises its owner's biometrics (fingerprints, face, voice), creates metrics and logs, and is highly programmable by millions of apps, many of which update automatically. It synchronises and shares data with other objects such as car entertainment systems (e.g., to enable hands-free calling and audio playback). It can track and be tracked by similar mobile devices in real-time. Its sociological importance is assured because it contains mountains of personal information. It is, for example, an invaluable source for profiling and evidence in police investigations. Further, from these logs are derived data for metrics, statistics, alerts, diagnostics, post-mortems, etc. Although there are standards and tools for logs, they are commonly customised to the software component they monitor [48].

Computer monitoring yields insights into the technicalities, working methods, culture and governance of monitoring as general phenomenon. This is because our lives are held together by software and data.

3. An Abstract Definition of Monitoring

The general working principle for our study is:

> *Monitoring is the collection, evaluation, recording and storing of data obtained from observing the behaviour of entities in a context. Behaviour is described by data and what is observed are properties of data. The outputs of monitoring are records containing judgements about these properties of data.*

Thus, we assume that monitoring is only concerned with data, and so our theory begins as a *theory of data*. Further, by data we have in mind information that can be represented digitally.

With a wide range of contexts and examples in mind, we begin to identify the essential components of monitoring:

Definition. Abstractly, a *monitoring process or system* consists of the following components:

1. ***Entity.*** Entities are people, or physical or virtual objects, that possess behaviour in space and time.
2. ***Identity.*** Methods for generating data that can identify entities and situate them in space and time.
3. ***Measurable behaviour.*** Methods for generating data that represent the actual behaviour of entities in space and time.
4. ***Attributes.*** Methods for describing, recognising and judging properties of measurable behaviour data.
5. ***Processing.*** Methods for analysing properties of the behaviour data and generating new data such as summaries and comparisons.
6. ***Recording and reviewing.*** Methods for storing and displaying data, properties and judgements for subsequent review and interpretation.

Each case of monitoring has a context that we define explicitly by the following:

7. ***Context.*** The collection of the chosen entities and behaviours, their data representations, and attributes of the data to be observed and judged, constitute a context.

The context takes shape through the choice of behaviours of interest, and the choice of what data represents them; in turn, the choice of data is shaped by the means to obtain it. The measurable data abstract a few features of the behaviour of the entity, and becomes a proxy that replaces the actual behaviour. In our model, we leave open the human procedures and technological infrastructure by which the data comes into existence.[7]

[7] The process of choosing data is outside our analysis, belonging to measurement theory, broadly conceived.

The act of observation in monitoring is the checking, or evaluating, or judging of *some* attributes of the data. So, what is actually monitored are *chosen* properties of the data *chosen* to represent *chosen* behaviours. Attributes can be derived from behavioural conditions, such as rules, norms, practices, targets and performance indicators, or determined by the technical state of the data and its measurement. Attributes can depend on time and space. Attributes may not be clearly present or absent, but their likelihood may be approximated or estimated; the attributes can be little more than beliefs about behaviour. The monitoring process records observations, nothing more. Our definition aims to reveal and capture a common 'anatomy' for diverse monitoring processes.

There is no shortage of areas where monitoring is orthodoxy. For example, accounting and auditing are monitoring processes that shape the management of an organisation, by which reports must be returned to a regulatory body. Let us illustrate these components, with simple examples in employment, retailing and criminal justice, where monitoring is explicit and acceptable.

Example 1: Management Key Performance Indicators. A key performance indicator (KPI) is a type of data designed to measure and track the performance of a person, process, service or organisation. Managers create systems based on KPIs to monitor and evaluate the success of activities, where success may mean conformance to standards, or progress toward objectives and targets. In Section 2.4 we mentioned manufacturing, warehousing and services where KPIs thrive and possibly rule. To these can be added public services which have long immersed themselves in targets and KPIs that are the subject of media attention and political disputes, e.g., in health and education.

Choosing KPIs defines a monitoring process for specific managerial objectives, which may be directed at the short-term behaviour of people or processes, or at long-term corporate goals. KPIs can have a hypnotic effect and in many situations the KPIs completely define, implicitly or explicitly, performance. Typically, a *dashboard* refers to a user-interface for the data that is current, concise and easy to interpret. The data displayed define indicators that are intended to allow instantaneous appreciation of current situation and progress. The *balanced scorecard* card is a popular form of dashboard [51].

For a simple example to illustrate the components, university key performance indicators for teaching might include:

1. ***Entity***. Teacher.
2. ***Identity***. Staff name, number and unit.
3. ***Measurable behaviour***. For each module taught: number of students enrolled; marks awarded; attendance and engagement; student opinions; student response.
4. ***Attributes***. For each module taught: classifications of data and profiles.
5. ***Processing***. Judgements of student performance against module averages, passes and fails, subject benchmarks, and management targets for progression.
6. ***Recording and reviewing***. Data for staff professional development review.

This can be extended to include staff research performance (e.g., papers published, grants applied for, research students supervised, esteem, external engagement, etc).

Example 2: Recommendation Systems. A retailer's recommendation system makes suggestions to customers about what they might be interested in buying, based on their history of purchases, patterns surrounding their products, and what might be inferred from this data. Familiar examples are supermarket recommendation systems based on loyalty cards. Retailers' data gathering for recommendations have been at the forefront of commercial monitoring applications and big data [52].

For online retailers, the monitoring opportunities are vastly improved with *much* more data easy to collect. Suggestions to account holders can be based on casual browsing as well purchase data. Amazon is the pioneer with its spectacularly influential recommendation algorithms, which are now more than 25 years old and widely deployed [53]. In the case of online retailing, the components of our definition may be illustrated as follows:

1. ***Entity***. Customer accounts.
2. ***Identity***. User names and passwords.
3. ***Measurable behaviour***. Purchasing profile: histories of purchases, product searches, page visits, responses to invitations.
4. ***Attributes***. Products purchased or considered as classified by tagging systems.
5. ***Processing***. Analysis of attributes, and generation of related and popular products.
6. ***Recording and reviewing***. Methods for storing the updated purchasing profile for subsequent recommendations and special offers.

Recommender systems are deployed in various media, sometimes with harmful consequences (e.g., in the death of Molly Rose Russell, aged 14 years old [54]).

Example 3: Electronic Monitoring: Penal Sanction. Currently, various forms of electronic monitoring (EM) are used to supervise offenders in the criminal justice process, e.g., at the pre-trial (bail), community penalty, and post-release stages. An EM-curfew seeks in some degree to prompt responsible, law-abiding behaviour at least for the duration of the curfew; it can also provide victim protection. For the purpose of restriction to places and times, EM takes a form of location monitoring, which uses sensors to secure compliance with a required routine sustained over a set period of time – in this instance, the curfew and its associated rules. For example, EM has remotely monitored chemical properties, such as alcohol and drug levels [55]; a curfew and restriction for drink driving consists of:

1. ***Entity***. Offenders.
2. ***Identity***. Names and numbers.
3. ***Measurable behaviour***. Data about offender location and alcohol consumption.
4. ***Attributes***. Presence and required actions at locations and times.
5. ***Processing***. Analysis of time entering and leaving a fixed location; results of skin tests for blood alcohol levels.
6. ***Recording and reviewing***. Data for offender review and management.

4. A General Definition of Monitoring with Interventions

A monitoring system produces data, but what is done with this data can vary enormously. In simple terms, the records *contain judgements on the degree that attributes are present in the data.* Monitoring designed to only record data is common – typical examples are polls and surveys. The data and statistics obtained may be private, or made public and end up in league tables.

However, the judgements can trigger processes or consequences that we call *interventions*. Interventions might aim to flag certain behaviours, or to notify and change behaviours of entities. For example, suppose the purpose of a monitoring system is to establish and sustain performance. When the data is reviewed, and if performance is found to be unsatisfactory, appropriate actions may to try to change behaviour and restore or improve performance. Such actions define use of monitoring. Interventions connect monitoring with *purpose*, which is fundamental in David Lyon's definition of surveillance.

Definition. Abstractly, a *monitoring process or system with interventions* is a monitoring system (as defined in Section 3) to whose components is added:

8. ***Intervention.*** Methods for reviewing and interpreting judgements and taking actions that are designed to notify or change the behaviour of the entities being monitored.

The interventions may take place at a place and time far from the monitoring process. To support security, cameras have long been installed in buildings to register movements; they need not trigger interventions. But, if something was wrong (e.g., unauthorized access or stealing), images stored may be used much later on as evidence that trigger action.

Thus, to passive monitoring, through interventions we add active monitoring, of which there will be many types. The interventions just mentioned for security cameras are examples of *retrospective interventions*. Other interventions are designed to respond to the present, such as used by speed cameras monitoring traffic. These we call *prospective interventions*. An architecture of the process is summarised in Figure 1.

Through interventions, possible or actual, concerns about trust, privacy, identity, etc. rapidly surface and lead to a host of questions about monitoring contexts, data and algorithms; it is from the contexts to which monitoring belong social concerns derive their meaning [56]. A theory of monitoring with interventions can becomes a precision tool for analysing surveillance.

Clearly the nature, timing and purpose of the interventions are important parameters in making a typology for monitoring. We exemplify our idea of monitoring system with interventions by reflecting on five basic types of monitoring for the purposes of: (i) access control; (ii) permissions; (iii) penalties; (iv) incentives; and (v) recommendations. A monitoring system can belong to more than one type, e.g., access and permission, or penalty and incentive. For real-world examples, there are also options to choose where the work of the monitoring system ends, and where that of the intervention system begins.

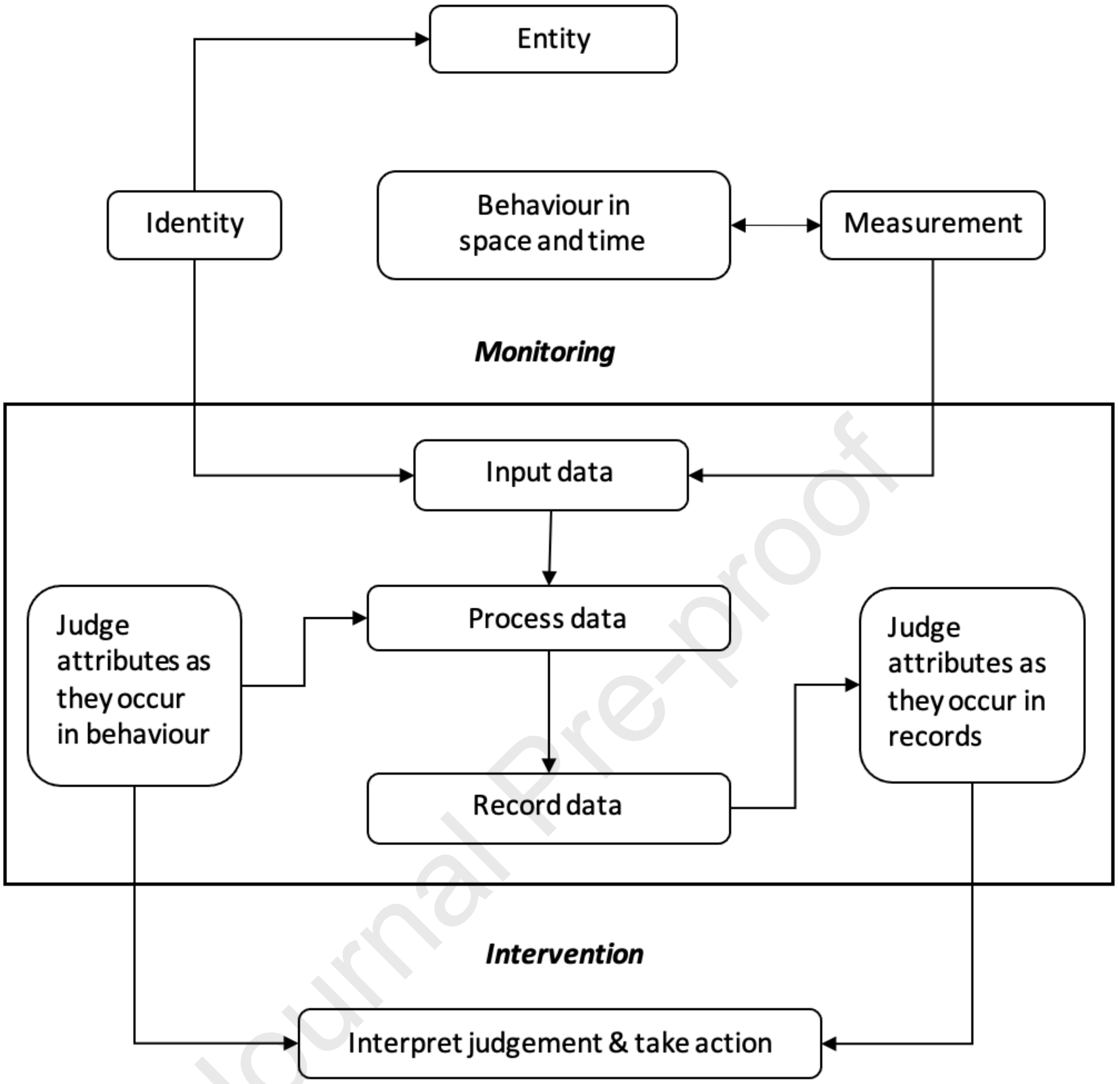
Entity
Identity
Behaviour in space and time
Measurement
Monitoring
Input data
Judge attributes as they occur in behaviour
Process data
Judge attributes as they occur in records
Record data
Intervention
Interpret judgement & take action

Figure 1: Monitoring with interventions

4.1. Access control systems

We conceive of an *access control system* as consisting of two parts: (i) a monitoring system that observes entities by checking their data against conditions that allow them to gain immediate access to a set of resources (e.g., a location, an event, a list of services, files, etc.); and (ii) an intervention system that uses the information produced by the monitoring system to enable or prevent the entity's access to the resource. The information produced by the monitoring system for access is, typically though not exclusively, a binary decision – yes/no, in/out, open/close, etc.

Prominent examples of access control systems are electronic lock systems, based on programmable plastic cards as keys; plastic ticketing cards (e.g., travel cards such as the Oyster card in London and MetroCard in New York); systems with logins and passwords (e.g., ATMs, computers, photocopiers, phones, online accounts of all kinds). In each case, systems record who has what access and when. Increasingly, access control systems are aided by biometrics of the finger, face, voice, etc. [57]. In each case, acceptance or rejection is a result. However, the rules of access control, contained in the attributes in a monitoring system, are highly contextualised. They can depend on space and time (e.g., traffic congestion charges; entry into buildings at set times). They can be hierarchical, like lock systems with master and sub-master keys, or operating systems that enable files to be read but not edited. The confidentiality of computer files for the defence and security services led to complicated mathematical models of hierarchical access, starting in 1973 with *Bell-La Padula models* [58].

In the case of passwords there are many login scenarios which need the intervention component. For example, a simple password system to an ATM consists of:

1. ***Entity***. People using a specific ATM.
2. ***Identity***. Account numbers and card codes.
3. ***Measurable behaviour***. Input of four-digit pin numbers.
4. ***Attributes***. The registered pin numbers.
5. ***Processing***. Matching the registered pin numbers; counting failed attempts.
6. ***Recording and reviewing***. Storing the date, time and decision of the transaction.
7. ***Intervention***. Invitation or rejection to use the banking services available; blocking further attempts if more than (say) five failed attempts.

4.2. Permission Systems

Access to a resource does not always imply permission to use the resource. Consider the ATM: as an assess control system, it may (or may not) provide the access to the banking service via a card and a pin-number, but access does not give permission to withdraw any sum of money. The ATM is a gateway to other ‘backend’ monitoring systems.

We conceive of a *permission system* as consisting of two parts: (i) a monitoring system that observes entities and confirms that their data meet conditions that enables them to possess or use a resource (e.g., a service); and (ii) an intervention system that uses the information produced by the monitoring system to deliver, modify, or prevent the entity’s possession and use of the resource. Clearly, all access control systems are forms of permission systems; indeed, many permission systems are guarded by access control systems.

Prominent examples of permission systems can be found in operating systems of computers (e.g., Unix families), security management frameworks for organisations (e.g., role-based security), and licensing arrangements (e.g., for drivers and motor vehicles). The rules of permission, contained in the interventions of a monitoring system, are highly contextualised and dependent on time/space.

Central to most computer operating systems is the idea of a file, which to a user typically contains texts, sounds or images. Operating systems can specify which users or computer programs are granted access to a file, and what operations are allowed on it (e.g., files can easily be password ‘protected’ or ‘read-only’).

The security framework *role-based access control* **(**RBAC) is widely used by commercial organisations. It is general and capable of mathematical description, like its origins in Bell-LaPadula [58]. Unlike a simple access control system, RBAC associates permission with roles within an organisation. A role is a collection of jobs and functions. A member of an organisation has (i) a set of *authorised* roles, which he/she is allowed to fulfil at the same or different times; and (ii) a set of *active* roles, which he/she currently occupies. Roles have an associated set of transactions, which are the specific activities that someone in that role is permitted to carry out. In RBAC there are three primary roles: (i) *role assignment*: a person can exercise a permission only if the person has selected, or been assigned, a role; (ii) *role authorization*: a person's active role must be authorized. Role assignment ensures that people can take on only roles for which they are authorized; and (iii) *permission authorization*: a person can execute a permission only if the permission is authorized for the person's *active* role. In conjunction with (i) and (ii), this rule ensures that users can exercise only permissions for which they are authorized. Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles. A user may have multiple simultaneous sessions with different permissions.

Licensing of cars and their drivers are permission systems. In the UK, each car must be registered to a person called the keeper. For the car to be driven legally on public roads, the keeper must have a current road fund licence for the car; such a license can last six or 12 months. The cost of the road fund licence depends on the car, and it is essentially a tax that supports transport (as its name suggests). To purchase the licence for the car, which is the permission needed for the car to be driven, the keeper must have two further forms of permission: (i) a current certificate of road worthiness (if the car is more than three years old); and (ii) a current certificate of insurance for the driver. The licensing of drivers is a process that gives permission to individuals to be allowed to drive. It specifies what types of vehicles, medical conditions, and a record of motoring offences (points). This latter feature plays a prominent role in interventions: as the points mount up the validity of the driving licences declines. Licensing pioneered the creation of big data centres in the late 1960s [59].

Returning to the ATM, some services are available on access (e.g., ways of viewing the balance of account); others are governed by further permissions (e.g., availability of funds). To illustrate:

1. ***Entity***: People using a specific ATM.
2. ***Identity***: Account numbers and card identity codes.
3. ***Observable behaviour***: Four-digit pin numbers and cash withdrawal requests.
4. ***Attributes***: The registered pin numbers and account balance.
5. ***Processing***: Matching the registered pin numbers and checking the availability of funds.
6. ***Recording and reviewing***: Storing the date, time, decision and amount of the transaction.

7. ***Intervention***: Access to the banking service or not, delivering the cash or not, and updating the account or not.

4.3. Penalty System

We conceive of a *penalty system* as consisting of: (i) a monitoring system that observes entities and confirms that their data do or do not conform to some set of norms, rules or laws; and (ii) an intervention system that reviews the information produced by the monitoring system to possibly issue a penalty for non-conformity.

Simple examples of penalty systems are login scenarios where access is delayed or suspended after a fixed number of failed attempts at entering a pin or a password. There are plenty of examples of penalty systems to do with cars: parking systems, for which interventions are parking fines, and minor driving offences, for which interventions are points added to driving licenses. Advanced examples of monitoring with penalties are realised in pilot projects in China, such as the use of cameras with facial recognition monitoring the streets. Pedestrians disobeying lights at road crossings can be observed and interventions can identify them in databases and display their face. Less minor is electronic tagging of offenders on probation. Revisiting example 3 in Section 3, we can simply add the following intervention:

7. ***Intervention***: Warning or return to custody.

4.4. Incentive System

We conceive of an *incentive system* as consisting of: (i) a monitoring system that observes entities and confirms that their data do, or do not, conform to some set of expectations/norms/rules; and (ii) an intervention system that uses the information produced by the monitoring system to reward or improve performance. Some examples of incentive systems are professional development reviews for staff in organisations, guided by expectations of their grades, for which the interventions in these cases may be promotions and financial bonuses; and, in companies, monitoring sales targets, for which interventions may be training or a change of targets. Incentive systems are closely related to penalty systems. In certain circumstances, the absence of a penalty is an incentive, and the absence of a reward is a penalty.

Dramatic examples of monitoring with interventions that are both incentives and penalties are pilot projects for the conception of the Chinese social credit system, announced in 2014 [60]. A wide spectrum of commercial and state monitoring systems delivers personal data that can be aggregated and scored to reflect performance as a citizen. High social credit scores bring opportunities for the citizen, low social credit scores remove them [61]. For a useful introduction and reflection, see Zuboff [5: 388-394].

Simply revisiting example 1 in Section 3, we can simply add the following intervention:

7. ***Intervention***: A change of teaching duties.

4.5. Recommendation System

We conceive of a *recommendation system* as consisting of: (i) a monitoring system that observes entities and classifies their data into some pre-defined categories; and (ii) an intervention system that uses the information produced by the monitoring system to give a recommendation, suggestion, advice, or warning. A simple example would be an electronic speed limit sign that displays the actual speed of an approaching motor car, if travelling at more than the speed limit. Examples abound in online retailing, where a user's browsing can lead to the retailer sending emails suggesting products sometime after making a purchase or visit. For example, revisiting example 2 in Section 3, we can add the following intervention:

7. ***Intervention***: Making a recommendation or special offer.

5. Conclusion

5.1 Reflections

In conclusion, we have formulated and explored some general foundational questions about the nature of monitoring. An objective is to point to the significance and reach of the *idea* of monitoring, and to open up and call for research about monitoring and its influence and effects. Our approach is to focus and build on the technical nature of monitoring *as it is determined by* *the digital systems that create, manage and use data.* Other approaches are to be welcomed and will be needed.

Evidently, monitoring is encouraged by powerful forces – established practices in employment; commercial data analytics; corporate strategies for data as commodity and as capital; regulation and governance; evidence, transparency and accountability in public affairs; situation awareness for disaster management and military operations; security threats at large in the world. Some of the effects on people raise concerns and controversies, but by no means all. The benefits and problems of monitoring are determined by application domains and, indeed, whole hierarchies of contexts within those domains [cf. 56] and, of course, the cultural attributes of nations [cf. Kao and Sapp 2022].

However, our focus is a *technical* force encouraging monitoring: software's capabilities for automatically collecting and sharing data are changing the scope, depth and scale of monitoring on a daily basis. In this paper, we have touched on monitoring in the technical worlds of data science and digital technology; in the socio-economic world of employment, where monitoring is an orthodoxy; and in the open-ended social world of individual life, where surveillance thrives. We claim that the nature and roles of monitoring *per se* are significant, and need study and debate. To establish monitoring's theoretical independence, and to help analyse its many manifestations, we have proposed two abstract concepts of monitoring (without or with interventions) in which data collection and use are separated, and we have started building a set of typologies.

5.2 Future research

Some recommendations for further research arising from this paper are to: (1) explore monitoring's conceptual role in some existing areas of study and debate; (2) develop general abstract theories of monitoring; (3) take on some empirical challenges to develop and test theories through their application and customisation.

Mapping its influence. There are many areas to explore and map the role of monitoring. Structured social contexts, such as employment, governance, criminal justice, and healthcare, have conformance monitoring deeply rooted in their philosophies, culture and operational practices. And there are new areas emerging, such as private life where the idea of the 'quantified self' is all about monitoring [63]. Let us comment on employment and governance.

Employment and Management. In the world of business, monitoring is an *idée fixe*. It has been for more than a century since the 20th Century workplace was transformed by the radical scientific philosophy and practical methodologies of Frederick W Taylor (1856 –1915) and his collaborators and acolytes: Barth, Gant, the Gilbreths, Ford. To these who transformed manufacturing productivity must be added the less celebrated Henry William Leffingwell (1876-1934), who began the transformation of service industries with studies of office work [64]. Taylor's seminal work, *The Principles of Scientific Management* remains influential and interesting [65, 66]. Metrics and conformance monitoring to control performance and productivity is at the heart of Taylorism.

Digital technologies have automated monitoring metrics in the workplace. A seminal study of the unique nature of information technology in the workplace of the 1980s is Shoshana Zuboff's *In the Age of the Smart Machine* [67]. This exploration is a treasure chest of ideas, observations and field work and has the makings of a general theory – as the forensic analysis in Burton-Jones [68] demonstrates – one that now needs to accommodate three decades of technical change. Simon Head's *The New Ruthless Economy* [69] provides an overview of workplace practices of two decades later, also based on fieldwork and grounded historically in Taylorism. Like Zuboff, his focus is the unique role of information technology in (re-)making the workplace. To shape and standardise much of the *global* workplace, companies use enterprise resource planning (ERP) software, such as that sold by SAP and IBM. ERP software is embedded with monitoring functions, which have become essential to managing companies. When Head returns to the subject a decade later in *Mindless*, the driving role of monitoring is more evident [70]. The intensification of monitoring in the workplace calls for a novel theory of *Digital* Taylorism.

Governance. In matters of governance, monitoring is also an *idée fixe.* It provides evidence, transparency and accountability. An important socio-political context is regulation and government, where the theoretical and empirical work of Christopher Hood is a modern foundation for a study of monitoring. His 1983 analysis of *the tools of government* owes much to technology, as the notions of *directors*, *detectors* and *effectors* come from cybernetics. In particular, his detectors are 'a set of tools for examination, inspection, monitoring, watching and detecting, tools which must be applicable to a wide range of objects' [71, Chapter 6: 91]. His later studies of risk regulation also have cybernetic credentials with its standards, monitoring and change. Thus, like Zuboff on employment, Hook on governance is a foundation for deeper studies of monitoring with digital technology in focus [cf. 72]. However, these themes of policy, governance and regulation also lead to the rise of the empirical epistemology mentioned earlier [18, 19].

Developing theory. Of course, a possible new debate stimulated by our paper is on the value of theorising monitoring, on distinctions to made between monitoring and surveillance, and the grey areas in between, and on its usefulness. Our position on monitoring is that in order to make progress on the well-established study of surveillance and its effects, the world of digital data and technology upon which it depends needs to be explicit and to receive deeper analytical attention.

Turning to future technical work, monitoring data has a natural hierarchical structure that theory needs to capture and analyse. Some obvious levels in the hierarchy include raw data at source; new data computed and/or inferred from previous data; categories that interpret, classify and tag data; metrics and units with which to calibrate and compare data; and triggers for action and change. This research programme could aim at a comprehensive ontology that can be used to think about old and new roles for monitoring and their effects. For example, a theory of monitoring can shed light on *technical* issues of privacy. The problem of controlling the *use* of personal data – possibly constructed from ingenious correlations and deductions based on aggregations of independent data sets – can be tackled by a system of provenance of information. This requires monitoring where data comes from, in order for its use to become transparent and accountable with respect to laws and regulations [73]. An attempt at a monitoring ontology is best rooted in a particular domain.

To connect with the software that underpins monitoring, a research programme could aim at a formal theory of monitoring with mathematical models of monitoring systems and interventions, made using algebra and logic. The models could help clarify design decisions in system development and be used as a tool for system certification. Our abstract definitions and typologies are a basis for such a mathematical development.

Field work. A monitoring theory is tool to examine the origins and processing of data sets, and to give a technical insight or perspective on motivations, ethical implications, and active uses and misuses. Our theoretical concepts can be used to design a methodology for studying monitoring ‘in the wild’. Fieldwork would benefit from a conceptually well-founded framework, that can

(i) demand clarification and precision in what data is gathered;

(ii) develop precise concepts and common terminology;

(iii) inform the differentiation and classification of data;

(iv) recognise and compare features in disparate situations;

(v) discover new characteristics, abstract concepts or problems that may be of wide relevance; and

(vi) map accurately changes in past, present and future practices.

In addition to the areas suggested earlier, other rewarding areas of ‘the wild’ in which to study monitoring could be added are our urban and domestic worlds as they are re-shaped into ‘smart’ cities and homes [74, 75].

References

[1] Laney D (2001) 3D Data Management: Controlling Data Volume, Velocity and Variety. META Group. Available: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.
(accessed 14 November 2022).

[2] Galič M, Timan T & Koops BJ (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30(1): 9-37.

[3] Sadowski J (2019). When Data is Capital: Datafication, Accumulation, and Extraction. *Big Data & Society* 6(1): 1-12.

[4] Sadowski J (2020). *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*. The MIT Press.

[5] Zuboff S (2019). *The Age of Surveillance Capitalism*. Profile Books.

[6] Zuboff S (2016). The Secrets of Surveillance Capitalism. Frankfurter Allgemeine, Feuilleton. Available at: https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html
(accessed 14 November 2022).

[7] Lyon D (2007a). *Surveillance Studies: An Overview*. Malden, MA: Polity Press.

[8] Lyon D (2007b). Surveillance as Social Sorting.
Available: http://www.youtube.com/watch?v=xtAa-f-1rTg. (accessed 14 November 2022).

[9] Lyon D (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

[10] Attard J, Orlandi F, Scerri S &Auer S (2015) A systematic review of open government data initiatives. *Government. Information Quarterly*, 32(4): 399-418.

[11] Hunt M (2020) UK's Cabinet Office wins back government data brief after two-year hiatus. *Global Government Forum*, 24 July, 2020.

[12] Kitchin R & McArdle G (2016) What makes big data, big data? Exploring the ontological characteristics of 26 datasets. *Big Data and Society* 3: 1-10.

[13] Patgiri R & Ahmed A (2016) Big Data: The V's of the Game Changer Paradigm. In: *IEEE 18th International Conference on High-Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, IEEE Computer Society, 17-24.

[14] Kitchin R (2013) Big data and human geography: Opportunities, challenges and risks. *Dialogues in Human Geography* 3: 262-267.

[15] Kitchin R (2014) Big data, new epistemologies and paradigm shifts. *Big Data and Society* April-June: 1-12.

[16] Hey T (2009) *The Fourth Paradigm: Data-Intensive Scientific Discovery*. Microsoft Research.

[17] Lazer D, Pentland A, Adamic L, Sinan A, Barabási A-L, Brewer D, Christakis N, Contractor N, Fowler J, Gutmann M, Jebara T, King G, Macy M, Roy D, & Alstyne MV (2009) Computational Social Science. *Science* 323(5915): 721-723.

[18] Rieder G & Simon J (2016) Datatrust: Or, the political quest for numerical evidence and the epistemologies of Big Data. *Big Data & Society, 3*(1), 1-6.

[19] Rieder G & Simon, J (2017) Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences. In: Pietsch W, Wernecke, J, Ott, M (eds) *Berechenbarkeit der Welt?*. Springer VS, Wiesbaden.

[20] Deluze G (1992). Postscript on the societies of control. October, 59, 3-7.

[21] Haggerty, KD & Ericson, RV (2003). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–22.

[22] Sætra HS (2020), Privacy as an aggregate public good, *Technology in Society*, 63 (2020), 101422.

[23] Sætra HS (2019), Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defence of privacy in the era of Big Data, *Technology in Society,* 58 (2019), 101160.

[24] Haggerty, K (2006). Tear down the walls: on demolishing the panopticon. In D. Lyon (Ed.), *Theorising surveillance: The panopticon and beyond* (pp. 23 – 45). Portland: Willan Publishing.

[25] Fuchs, C (2013). Political economy and surveillance theory. *Critical Sociology*. 39 (5), 671-687.

[26] Bellamy Foster J & McChesney RW (2014). Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, 66(3).

[27] Zuboff S (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, 75–89.

[28] Lupton D (2013a). Types of veillance relevant to digital sociology. Available: https://simplysociology.wordpress.com/tag/veillance.

[29] Lupton D (2014). *Digital Sociology*. Routledge.

[30] Morgan, H (2014). Surveillance in contemporary health and social care: friend or foe? *Surveillance & Society* 12(4): 594-596.

[31] Mann S, Nolan J & Wellman B (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1(3): 331-355.

[32] Lupton D (2013b). Quantifying the body: monitoring and measuring health in the age of mHealth technologies. *Critical Public Health* 23(4): 393-403.

[33] Cecchinato, ME, Gould, S & Pitts, FH (2021). Self-Tracking & Sousveillance at Work: Insights from Human-Computer Interaction & Social Science. In P. Moore, & J. Woodcock (Eds.), *Augmented Exploitation: Artificial Intelligence, Automation, and Work* Pluto Press.

[34] Sheridan, C (2016). Foucault, Power and the Modern Panopticon. Senior Thesis, Trinity College Hartford, CT. Available: http://digitalrepository.trincoll.edu/theses/548

[35] Albrechtslund A & Ryberg T (2011). Participatory Surveillance in Intelligence Building. *Design Issues* 27(3): 35-46.

[36] Saheb T, Sabour E, Qanbary F & Saheb T,
Delineating privacy aspects of COVID tracing applications embedded with proximity measurement technologies & digital technologies, *Technology in Society*, 69, 2022, 101968.

[37] Ioannou A & Tussyadiah I (2021), Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours, *Technology in Society*, 67, 2021, 101774.

[38] Wang V & Tucker JV (2017). Surveillance and identity: conceptual framework and formal models. *Journal of Cybersecurity* 3(3/1): 145-58.

[39] Wang V & Tucker JV (2021). 'I am not a number': Conceptualising identity in digital surveillance, *Technology in Society*, 67, 101772.

[40] Xie S (2019). Using Smartphones to Pay? That's So Yesterday in China. *Wall Street Journal*, 10 June 2019.

[41] Bu QX (2021). The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review* 2: 113-145.

[42] Fontes C, Hohma E, Corrigan CC & Lütge C (2022), AI-powered public surveillance systems: why we (might) need them and how we want them, *Technology in Society*, 71 (2022), 102137.

[43] South Wales Police (2022). *Keeping South Wales safe with facial recognition technology*. Available: Keeping South Wales safe with facial recognition technology | South Wales Police (south-wales.police.uk) (accessed 14 November 2022).

[44] South Wales Police (2020). *Response to the Court of Appeal judgment on the use of facial recognition technology*. Available: Response to the Court of Appeal judgment on the use of facial recognition technology | South Wales Police (south-wales.police.uk)
(accessed 14 November 2022).

[45] Court of Appeal, Neutral Citation Number: [2020] EWCA Civ 1058. Case No: C1/2019/2670 (2020). Available:
Microsoft Word - R (Bridges) -v- CC South Wales _ors Judgment.docx (judiciary.uk)
(accessed 14 November 2022).

[46] Rosencranc L (2022), How to pick the right DEX tool for the best digital employee experience, Computer *World*, 27 September 2022. Available:
How to pick the right DEX tool for the best digital employee experience | Computerworld
(accessed 14 November 2022).

[47] Ashton K (2015). *How to Fly a Horse: The Secret History of Creation, Invention, and Discovery*. Penguin.

[48] Julian M (2017). *Practical Monitoring: Effective Strategies for the Real World*. O'Reilly.

[49] Dodge M & Kitchin R (2009). Software, objects and home spaces. *Environment and Planning A* 41: 1344-1365.

[50] Dodge M & Kitchin R (2011). *Code/Space*. MIT Press.

[51] Kaplan RS & Norton DP (1996). *The Balanced Scorecard: Translating Strategy into Action*. Boston, MA.: Harvard Business School Press.

[52] Lauer J (2020). Plastic surveillance: Payment cards and the history of transactional data, 1888 to present. *Big Data & Society* January-June: 1-14.

[53] Smith B & Linden G (2017). Two Decades of Recommender Systems at Amazon.com. *IEEE Internet Computing* 21(3): 12-18.

[54] Walker, A (2022) *Regulation 28 Report To Prevent Future Deaths*, North London Coroner's Service, 13th October 2022.
Available: https://www.judiciary.uk/wp-content/uploads/2022/10/Molly-Russell-Prevention-of-future-deaths-report-2022-0315_Published.pdf (accessed 14 November 2022).

[55] Nellis M (2009) Surveillance and confinement: Explaining and understanding the experience of electronically monitored curfews. *European Journal of Probation* 1(1): 41-65.

[56] Nissenbaum H (2019) Contextual Integrity Up and Down the Data Food Chain, *Theoretical Inquiries in Law*, 20 (1): 221-256.

[57] Vacca J (2007) *Biometric Technologies and Verification Systems*. Elsevier.

[58] Bell DE (2005) Looking back at the Bell-La Padula model. In: *Proceedings of 21st Annual Computer Security Applications Conference,* NW Washington DC, United States, 5-9 December 2005, pp. 337-351. IEEE Computer Society.

[59] Tucker JV (2015) *Big Data Comes to Wales. The Early Years of the DVLA: 1965-1975,* YouTube. Available: https://www.youtube.com/watch?v=SX_x0Lyua_Y
(accessed 14 November 2022).

[60] Creemers R (Translator 2015) Planning Outline for the Construction of a Social Credit System (2014-2020). *China Copyright and Media*.
Available: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (accessed 29 June 2021).

[61] Anonymous (2016) China invents the digital totalitarian state. *The Economist*. 17 December 2016.

[62] Kao Y-H & Sapp SH, (2022) The effect of cultural values and institutional trust on public perceptions of government use of network surveillance, *Technology in Society*, 70, (2022), 102047

[63] Ajana B (2020) Personal metrics: users' experiences and perceptions of self-tracking practices and data, *Social Science Information*, 59(4): 654-678.

[64] Leffingwell WH (1917) *Scientific Office Management*, A. W. Shaw Company, Chicago.

[65] Taylor FW (1911) *The Principles of Scientific Management*. New York: Harper and Bros. Reprinted New York. Dover Publications

[66] Wren D (2011) The centennial of Frederick W Taylor's The Principles of Scientific Management: A retrospective commentary. *Journal of Business and Management* 17(1): 11-22.

[67] Zuboff S (1988) *In the Age of the Smart Machine: The Future of Work and Power*, Basic Books.

[68] Burton-Jones A (2014) What have we learned from the Smart Machine? *Information and Organization*, 24: 71–105.

[69] Head S (2003) *The New Ruthless Economy: Work and Power in the Digital Age*. OUP USA.

[70] Head S (2014) *Mindless: Why Smarter Machines are Making Dumber Humans*. Basic Books.

[71] Hood, C (1983) *The Tools of Government*, Macmillan Press.

[72] Hood, C and Margetts, H (2007) *The Tools of Government in the Digital Age*. Palgrave-Macmillan.

[73] Weitzner D J, Abelson H, Berners-Lee T, Feigenbaum J, Hendler J & Sussman G J (2008) Information accountability. *Communications of the ACM,* 51: 82-87.

[74] Gubbi J, Buyya R, Marusic S & Palaniswami M (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29: 1645-1660.

[75] Whitmore A, Agarwal A & Xu LD (2015) The Internet of Things - A survey of topics and trends. *Information System Frontiers* 17: 261-274.

People watching:
abstractions and orthodoxies of monitoring

- Monitoring is explored as an independent subject area.
- Monitoring as a process that observes people or objects.
- Information recorded by monitoring can initiate actions named interventions.
- Interventions that specify or reveal what the monitoring data is used for.