‘I am not a number’: Conceptualising digital identity in digital surveillance

Victoria Wang, University of Portsmouth

John Tucker, Swansea University

Abstract

Surveillance, now a commonplace phenomenon in everyday life, has been explored from various disciplines over three decades. Today’s surveillance practices depend primarily upon many software technologies that collect, store and process personal data for the purposes of influence, management, protection or detection. The identification and categorisation of data have thus emerged as the technical signature of surveillance. An individual has many identities belonging to different contexts of his/her life, but in this paper, we explore the relationship between surveillance and identity in virtual contexts only. We argue that an understanding of identity purely as data is fundamental to understanding surveillance. We propose abstract general definitions of surveillance and identity that together create a conceptual framework, capturing key features common to many disparate surveillance situations. Our work concludes that the essence of surveillance is that of a *surveillance context*, which is precisely and solely defined by the availability of data about the behaviour and identity of its entities. The data that distinguishes the entities of the context we call *identifiers*; we explore the *creation*, *provenance*, *comparison* and *transformation* of identifiers. Abstractly, surveillance is a process that tests for properties of data, and sorts identifiers into categories.

Key Words: surveillance, identifier, monitoring, software, social sorting, digital society

1. Introduction

In the iconic 1967 television series *The Prisoner*, Patrick McGoohan popularised the assertion 'I am not a number. I am a free man'. The series perplexed audiences by its themes of covert rendition, surveillance, and anonymity delivered by advanced technologies of control, in an idyllic unreal village. The inhabitants of the village are known by numbers; and their once secretive lives are under constant observation and demands for information by obscure authorities. The allegory thrives, 50 years later, as surveillance and identity have weaved themselves into the virtual fabric of everyday life. In our time, where data about all aspects of contemporary life is generated and encoded in binary numbers, we are known by numbers too.

Almost two decades ago, Lyon [1, 2, 3] made clear the nature and significance of contemporary surveillance, and the invisible influence of its social ordering effects in everyday life. Later, he gave a concise definition of surveillance as: "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or detection" [4: 14]. Its functions can be grouped into three categories: *control, social sorting* and *mutual monitoring* (ibid.). The main purpose of contemporary surveillance, which is dominated by software, is *social sorting,* which he defined as the "focus on the social and economic categories and the computer codes by which personal data is organized with a view to influencing and managing people and populations" [3: 2]. His definition builds upon the original model of social sorting, called 'panoptic sort' in Gandy [5], together with other critiques by Beck [6] on 'risk society'; Marx [7] on 'new surveillance'; and Ericson and Haggerty [8] on 'policing the risk society'.

Today, surveillance is an everyday experience. Using surveillance data, individuals are sorted into categories that influence their opinions, opportunities, treatment and actions [3, 9, 10, 11, 12, 13]. These sorting practices trade distinct real-world individual identities for conceptual group identities as criteria for decision-making.[1] Such sorting into groups are forms of identity construction. Thus, *identification* is at the heart of all contemporary surveillance practices [15, 16].

The term 'identity' can refer to different ways in which individuals and groups are distinguished in their political, economic and social relations [17], and is studied differently in various disciplines [18]. In the face of unrelenting technological developments, more and more sources of data are generated by our products, services and environments, which are becoming increasingly digital. Inferences from this data become explicit and accessible, and automated. Now, Lyon's [11] call, more than a decade ago, for cross-disciplinary research into the social implications of the new technologies for social sorting is even more pressing. However, to do this we need an appreciation of the technical foundations of surveillance: surveillance is shaped by the materials of data and software.

We propose that there is a need for a theoretical framework to explore the role of identity in contemporary surveillance practices delivered by software. Such a framework would surface and elevate technical concepts and have the following properties:

Theoretical Desiderata

[1] Commonplace historic examples are using risk profiles to cost insurance and allocate credit [14].

1. **Generality**. Its central concepts should apply to a wide variety of surveillance situations, allowing it to be customised to various domains/problems.
2. **Identity**. It makes explicit the nature and role of identity in surveillance practices.
3. **Sorting**. It analyses social sorting based on precise notions of identity.
4. **Comparison**. It allows different surveillance situations to be compared so that properties and observations about one help to illuminate others.
5. **Taxonomy**. It is able to build classifications of surveillance situations and their social implications.
6. **Precision**. It can be used to enhance precision in observation and conceptualisation in empirical case studies.
7. **Behaviour of interest**. It can be used to reveal underlying causes of behaviours of interest, such as violations of privacy, deceptions, and unintended consequences.
8. **Combining disciplines**. It can be used by different disciplines and can be developed as a platform with which to build cross disciplinary investigations.
9. **Invariance in the face of change.** It can be used over long periods of time and can apply to technical and social change.

A theoretical framework that meets these desiderata would be useful and new. In this paper, we attempt to develop such an abstract conceptual framework that is precisely defined in order to investigate surveillance in a way that emphasizes the role of identity. Conditions 1-4 can be demonstrated here; conditions 5-9 require subsequent specialised case studies.

In the matter of combining disciplines (condition 8), we think that building a theoretical bridge between social and political disciplines and computer science is the most challenging and urgent. Whilst everywhere there is academic encouragement of cross-disciplinary working, from our own experience, there is also some reluctance to allow the abstract and technical

concepts of computer science into social discourses.[2] These general concepts have been stripped of their origins, motivations and significance for people and require a style of exposition that prizes logical organisation and discourages nuance.

In the matter of change (condition 9), to understand the contemporary, and have a sense of possible futures, we need abstract concepts that offer views of historical continuities. Indeed, we need abstract concepts and general definitions – such as those of Lyon, Clarke and others on surveillance – capable of analysing the fast-changing phenomena of our information obsessed society.

First, we picture how surveillance and identity are evolving, and describe some of its roots in digital technologies to motivate our technocratic approach to surveillance. We then introduce our theoretical framework which is based on some abstract concepts that reveal a common structure for many disparate surveillance situations. Lastly, we outline the elements of theory of identity as data. Our approach is to separate people from their data, and to study only their data. We explore the following *Exclusion or Reduction Principle*:

> *In a surveillance situation, people and objects and their behaviour are observed and identified* ***only*** *through data; and the data that is collected completely defines the surveillance situation. In a surveillance situation, all that can be known about people and objects is what can be inferred from the data collected.*

[2] The framework we propose builds upon a preliminary mathematical study of surveillance and identity data [19].

Our Exclusion Principle focuses on data – the raw material from which digital traces of the activities of individuals are made. By data we mean numbers, texts, sounds and images, video, etc., ultimately encoded in binary. What is observed is data about behaviours, what is sorted is data about identities. Our abstract discussion is designed to analyse surveillance situations, now and in the future. Specifically, we formulate the abstract concepts of: (i) *surveillance context*, and (ii) *identifier* that distinguishes people and objects in the context. Then we propose that the theory must explore the *creation*, *provenance*, *comparison* and *transformation* of identifiers.

Of course, a theoretical framework that is general and precise will inevitably be abstract; and thus, at least to some, seem remote from the core issues of their interest in surveillance, which might be deeply focused on people in a particular domain, or with a social or political issue. But as general studies of surveillance have shown, surveillance is everywhere though seemingly diverse in its nature, purpose and consequences. Abstract frameworks may seem costly, especially when they are new, but they are ideal for unification as well as exploring the nature of, and keeping up, with change.[3] Furthermore, with their taxonomies, they may help answer questions such as:

- Is a surveillance system or policy technically effective, i.e., is it functioning correctly gathering and disposing of the right information?

or harder questions such as:

- Is a surveillance system or policy effective, i.e., is it achieving its goals for its owners and users?

[3] Our present hindsight and foresight can point out technological drivers of change such as: connectivity via the internet, smart phones, domestic products and environments.

Within these simple questions are the difficult notions of 'functioning correctly' and 'achieving goals'.[4]

An abstract framework can help us lay bare what data is collected and why. The data collected in surveillance is chosen – intentionally or unintentionally – and therefore must be explainable. The abstract framework is intended as a theoretical tool to help make transparency a requirement that is routine. Our framework reveals that there is indeed no such thing as pure, raw and unbiased data. Ideally, we seek specifications of surveillance systems and their purposes that enable us to better know and debate the scope and limits of surveillance situations.

The structure of the paper is this. In Section 2 we prepare the way for our theorising by reflecting on the literature. In Section 3, we describe and illustrate an abstract conception of for surveillance. Section 4 describes and illustrates an abstract conception identity, and in Section 5 we look at its intrinsic complexities. Section 5 offer some concluding remarks.

2. Background – Surveillance and identity in digital society

Of course, data processing applied to surveillance is not new. Data processing by punched cards was a mature technology in the 1930s and the basis of a global business, e.g., for IBM. To give an extreme example of the use of social sorting, IBM technology was used by the Third Reich to identify and locate Jews [21]. In contrast, the Stasi was less interested in computerising their extensive files [22]. Of course, surveillance practices do not need to be associated primarily with sinister conspiracies or dystopian images [23].

[4] See the discussion of such questions in intelligence community in [20].

Now, digital technologies are dominant not simply for processing data but as a primary means of collecting data, openly and covertly. The pervasiveness of software in everyday life is embraced by many, since they expedite individuals' daily lives in various ways, especially, in terms of shopping, travelling and socialising. An influential example is Amazon's invention of item-based collaborative filtering algorithms to recommend new products to customers based on what items they have purchased, placed in their baskets and wish lists, and especially on what other customers with similar interests have purchased [24]. Since 1998, these algorithms have been taken up by many retailers and service providers [25]. Facebook is an important source of personal data for companies and the world at large; Cambridge Analytica, digital marketing company notorious for its specialisation in politics, was one of many effective users of their data [26]. These are two among many global icons whose business is data collection.

In many cases, surveillance is the by-product or unintended consequence of other processes, as the systems that shape and hold together contemporary life are made with software. All software systems have surveillance capabilities since they naturally include tools that *generate, store and process data about their own operation.* Classically, operating systems that manage computers need logs for system maintenance. The collection of data about visits to websites is routine and comprehensive. The point is that *all software systems have the potential to be used as tools for surveillance*. For example, highly programmable by millions of apps, the smart phone manages itself, is location aware, and adapts to the environment.[5] Apps can collect all sorts of data in logs about their operation; since apps depend on other apps, the collection can be quite extensive and collaborative.

[5] The popular operating systems of Apple, Google and Microsoft are designed to collect, store and transmit data on users' physical locations to central databases without their consent [27].

Today, software is embedded in many domestic objects – cars, televisions, washing machines, etc. – and are networked to service providers and users, e.g., via their mobile phones. Dodge and Kitchin [28, 29] coined the term *logject* for objects employing software that monitor and record their own use. Technological developments like the internet of things (IoTs) are vastly increasing the number and distribution of logjects. For some, the infrastructure for Orwell's 'Big Brother' is already in millions of homes in devices, such as Amazon Alexa, or Google Home, etc., which continually monitor sounds in order to activate [30]. Speech and facial recognition technologies are creating a world of ubiquitous surveillance and identification.

Supreme examples of personal data sources are social media and messaging platforms, such as Facebook, Twitter, Instagram, WhatsApp, Snapchat, YouTube, and Weibo. Some of these social media platforms have evolved to include personal financial services that allow the receiving of funds, and the subsequent scanning of QR codes to pay for all sorts of products and services. For example, WeChat, released by Tencent in 2011, is a Chinese multi-purpose messaging, social media and mobile payment app. Seven years after its release, it became one of the world's largest standalone mobile apps, with monthly users passing 1 billion in February 2018 [31]. Due to is popularity and wide range of functions, it is used for mass surveillance by the Chinese government via various measures, e.g., scanning messages shared in WeChat and pulling them if they contain certain sensitive words or phrases [32].

Actually, in various social media platforms and cybercommunities, every word typed, and every movement made *can* be observed, recorded, stored, and replayed and examined in the future – In a complex cybercommunity, like Second Life, there is only data belonging to avatars and *perfect surveillance* is possible [33]. The idea of perfect surveillance is becoming relevant

and suggestive to the physical world too, as software invades and pieces together cyber-approximations of society.

Software's invasiveness needs not be subtle. As computer vision research advances, camera-based surveillance becomes prominent [34]. Of course, CCVT has long been a surveillance tool to deter anti-social and criminal behaviour, and upon which all sorts of police investigations have come to depend. Significant academic studies of the CCTV are long standing, e.g., [35]. Now, it is set to be revitalised with the addition of new recognition systems that can search and identify people in videos, and even categorise both their activities and emotions. Strikingly large-scale projects are well established in China that demonstrate some of this new surveillance capability.[6]

Certainly, software and computers collect, process and generate data that is fundamental to contemporary surveillance, and the main purpose of contemporary surveillance is simply the sorting of these data (condition 3). Therefore, one fundamental concept in contemporary surveillance studies should be identity and the data that represent identity. Identity is changing as smart buildings and cites expand throughout the world, whose communication networks have to authorise and authenticate devices of all kinds (e.g., robots and autonomous machines, physical infrastructures, cloud services, IoT installations).

[6] See: http://www.bbc.co.uk/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state . The news highlighted the start-up company SenseTime, whose facial recognition systems are involved:

Our approach is a technocratic one. Its focus on data resonates with Roger Clarke's notions of 'dataveillance' and 'digital persona'. The term 'dataveillance' refers to "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" [36]. The term 'digital persona' refers to "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual" [37]. His focus was on an organisation's need to identify individuals at a time when a network-enhanced world was emerging [38]. So, starting in Clarke [39], we find a remarkably perceptive and imaginative exploration of information systems. In Clarke [40], he reflects on the concept of 'digital persona' during its first 20 years, asserting that the concept had "insufficient impact to overcome the weaknesses in theory and practice that it was intended to address" [40: 182]. Since the coinage of 'digital persona' the world has been transformed by digital technologies.

In the wider literature, once a person's identity was assumed to be stable, natural and holistic [41]. Gradually, as sociological studies develop, identity becomes an influential and multi-layered concept, as in Goffman's seminal book *The presentation of self in everyday life* [42]. Later, concepts of identity flourish in social theories, especially in Giddens' *Modernity and self-identity* [43]. Here we find prescient conceptions of *faceless interactions* brought about by 'abstract systems' of various kinds – presumably trading with data. Today, a person's identity is more artificial, varied and fluid, and the subject of complex theories. The fragmentation of identity is promoted by people's engagement with a wide spectrum of digital services, which demand creating data about people and products. These demands have stimulated our appetite for data. Social theorists have been actively pursuing the consequences of this digital world, in general and especially in surveillance, e.g., [12, 44, 45, 46, 47, 48, 49]. Of particular importance is the technical role of identity in surveillance. In social terms, identity is fundamental to an

individual's control over the information they disclose about themselves in different situations [50].

Digital systems enable and encourage faceless interactions, which are fast replacing in person interactions in our fast-moving information society. To use these systems, an individual has to provide data to constitute his/her identity, distinguishing himself/herself from other users. The scale and diversity of the systems lead to the need for abstract notions. For example, 'data doubles' refer to many collections of personal data that represent you within a system [3]. Other examples are: 'dividaul' [51]; 'epers' [52]; 'shadow order' [53]; 'capta shadow' [54]; 'databased self' [55]; and 'Cyber-I' [56, 57]. These notions are common in surveillance studies where their terminology and interpretation reflect different contexts and scholarly purposes.

Some of these notions approximate the idea of an individual having what one might *loosely* refer to as a 'digital twin' – an idealised 'sum' of many and varied pieces of personal data that represent the individual in systems belonging to different bodies. These digital twins may include information that individuals have not created and cannot change. Their life cycles are subject to alteration, addition, amalgamation, inconsistencies and loss. Digital twins also risk immortality. Data is collected on such a vast scale that it is expensive to decide on what to delete or to keep. This natural tendency to hoard data is the target of privacy campaigns (e.g., the right to be forgotten) and data regulations (e.g., GDPR 2018). Through reproduction and transmission, digital twins have increased social plurality, and blurred public and private identities. They may have a life of their own, and so have a real influence on an individual's life chances and opportunities [58].

3. A general definition of surveillance

Surveillance includes processes that seem to belong to many distinct and incomparable situations, which make it difficult to tease out and make precise common patterns, classify phenomena, predict consequences. To counteract any tendency in surveillance to become a sundry collection of domain-specific empirical studies, our approach here is to develop a abstract framework that describes essential components of surveillance, and can be a general investigative tool and encourage the sharing of methods and insights. Despite the diversity of surveillance situations, the technological hard facts of the matter are that much *surveillance is made possible by, and has in common, the technicalities of data and software.* This observation is a prompt for our technocratic approach.

3.1 Surveillance contexts and sortings

To capture the structure of surveillance situations, we isolate and define some abstract concepts. The first key notion is a surveillance context:

A *surveillance context* consists of the following components:

1. ***Entity.*** Entities are people or objects that exhibit behaviour in space and time.
2. ***Behaviour.*** Behaviour of entities is observable through methods for creating and preserving data about behaviour.
3. ***Attribute.*** Behaviour is observed by methods for specifying and testing specific properties of behavioural data.
4. ***Identity.*** Identity is based on methods for assigning data to entities to name and distinguish them; the data we call *identifiers* for the entities.

The notion of a context is widely applicable as the range of entities, behaviours, attributes, and identifiers is vast. The attributes of interest can be based on any testable property. Putting entities into categories via chosen attributes is a process of classification. The idea of a context is used to define our second key notion:

Surveillance is a process that observes the behaviours of entities in a context. Observations are made by testing data provided by the context for chosen attributes. The attributes provide a basic classification of the data available; the attributes are chosen to detect only behaviours of interest which are specific to the data available in a context, rather than to any intrinsic nature of the entity. On recognising that the behaviour of an entity has an attribute, the surveillance process places *some* identifier(s) for that entity in the category defined by that attribute. Thus, consistent with the Exclusion Principle, surveillance systems output only data – identifiers – for entities that exhibit the attributes. The classification of identifiers for the entities is termed a *sorting*.

Thus, in general, *the natural form of an output of a surveillance system is a sorting of identifiers, which is a classification by attributes of the data available about the behaviour of entities in a certain context.*

The behaviours may satisfy several attributes and so a surveillance system can generate a classification by combining attributes in different ways; it may allow one category to be a subcategory of another with the result that a sorting that can have a hierarchical structure.

As we will see, the identifiers can be complicated and in working with a context we may need operations on identifiers. For example, three present themselves immediately: the *equivalence*

operation that given two identifiers tells whether or not they are associated with the same entity; the *search operation* that given an identifier finds a set of equivalent identifiers for the same entity – ideally, such an operation can find *all* equivalent identifiers; and operations that can create and delete identifiers for entities.

3.2 Some examples of contexts

Here are some simple examples of surveillance contexts to illustrate the idea is common to different surveillance situations.

On-line accounts. Commonly, the accounts we create – for shopping, banking, gaming, dating, socialising, and pontificating, etc. – have a common structure. There is a user name and password(s) to gain access to the account (also there could be custom numbers, multiple factor identification, biometrics). These act as a form of identifier the account. The account details establish a profile, which may be basic personal information (e.g., name, address, services chosen) or a fiction. The behaviour of an account is a history of interactions: logins, page use, financial transactions, queries, postings, conversations, or virtual activities of all kinds in online gaming and socializing communities, etc. For attributes, the account history can be subjected to regular or real-time monitoring, checking that terms and conditions are met by the client or if unusual patterns of interaction have taken place. For example, for a simple shop:

Entities: Customer accounts

Observable Behaviour: Transactions: service type, date, balance, payment, location, orders, returns, reviews.

Attributes: Payments, credit limit, relevant announcements/ads, unusual transactions

Identity: Account numbers

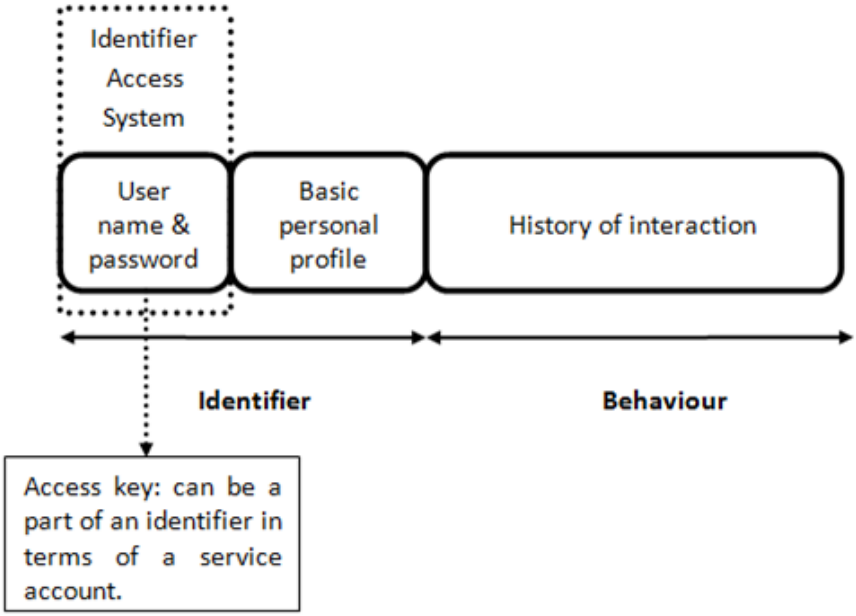

Figure 1: A typical online account

Smartphones. A smartphone is a mobile phone built on a computer with an operating system (e.g., iOS, Android and BlackBerry 10). A modern smartphone is an ideal tool for surveillance, having still and video cameras; a global positioning system (GPS); an accelerometer; biometrics; high speed data access. Last, but by no means least, it includes all kinds of apps, each of whose logs may be monitored. With these technical features (i) the activities of individuals, when carrying their smartphones, can be surveilled; and (ii) smartphones can be used by their owners to spy on others.

Consider (i). The technologies in the smartphone make it possible for the movement of the smartphone to be tracked to a high degree of accuracy. A constant stream of data is being generated and communicated by the smartphone to service providers. All kinds of properties of the user can be deduced from these data streams, including conversing, position and movement (e.g., running/walking/driving). In terms of our definition of a surveillance system, among many examples is a local search app for people, such as the 'People Nearby' function in WeChat:

Entity: Smartphones;

Observable Behaviour: Location of the smartphones running the app;

Attributes: Location within *n* kilometres;

Identity: A list of identifiers for individuals detected.

Consider (ii). Smartphones are commonly used in observing offenders (e.g., intelligence and evidence gathering); identifying risks to public safety; recording personal conversations and gathering otherwise hard-to-get data (peer-to-peer mutual monitoring) [59]. An individual can record an activity with a smartphone and stream the video live to a website. These rather direct forms of surveillance deliver data, which act as the start of independent processes for identifying people:

Entity: People or objects;

Observable Behaviour: Their actions;

Attributes: Perceived risks;

Identity: Images and sound.

3.3. Theoretical extensions

The above examples are simple in the sense that the data involved is familiar and precise. They show that the ideas are realized in huge range of surveillance situations. If an abstract framework can support explanations and accountability for what data is collected and why, then it will need to overcome the unfamiliar and imprecise too. Consider the ability to theorise about the basis of decision making about

(i) attributes and hence the classifications of behaviour; and

(ii) identities of entities in different roles.

In many surveillance situations decisions must take place in the presence of uncertain sources of information – data that is inexact, incomplete or fraudulent. A resilient framework must develop methods to allow for this uncertainty. The uncertainties of decision making are usually addressed theoretically by subtle logics, statistical estimates, probabilities, and degrees of belief. Increasingly, they are hidden away in AI systems.

4. A general definition of identity

What is the nature of the data used to represent identity of the entities in a context. Where does the data come from? What can be computed from the data by transforming, comparing and aggregating data? How is the data mapped to individuals?

4.1. On identifiers

By the Exclusion Principle, an entity's identity is purely a matter of data. Earlier, we defined an identifier as data associated with the entity, designed to distinguish it among other entities in a context. We have defined surveillance as a process that observes the behaviour of entities, and outputs sets of identifiers for entities with certain attributes. These identifiers may *narrow* the search for entities but need not contain enough information to pin down uniquely the particular entity under observation. Even when identifiers are very clearly chosen, the relationship between identifiers and entities in a context can be complicated [19].

Logically, four "ratios" of identifiers *versus* entities can arise:

1. ***One – One Associations***. Identifiers are assigned to one and only one entity.

2. ***Many – One Associations***. Different identifiers can be assigned to the same entity, but each identifier is assigned to only one entity.
3. ***One – Many Associations***. An identifier can be assigned to more than one entity but each entity has only one identifier.
4. ***Many – Many Associations***. An identifier can be assigned to more than one entity and, vice versa, an entity can be assigned more than one identifier.

These four are some simple properties that determine the usefulness of identifiers and are easily overlooked or taken for granted. Only in cases where the associations are one-one or many-one do identifiers point to a single entity, since in these cases *different entities have different identifiers*. In the one-one case, all information available in the context is contained in a single identifier. In the many-one case, identifiers may carry different information about a single entity; thus complete information about the entity that is available in the context is constituted by the set of *all* the identifiers of the entity. In cases of one-many and many-many associations, we need to know more to point to a single entity. Let us illustrate the distinctions by examples.

4.2 Everyday examples

Consider these examples that illustrate these ideas in everyday contexts. Standard one-one associations are the assignment of registration marks to motor vehicles, and phone numbers to mobile phones. One-one assignments are common when money is involved.

An obvious traditional one-many assignment is that of giving names to people: few names belong to only one person in a region; another one-many assignment is its generalisation of assigning passwords to online accounts, though usernames are usually one-one associations. An influential example of a one-many association is the assignment of postcodes to addresses

by the postal service: in the UK, commonly, each house has one postcode, but several houses share the same postcode. An example of a many-many association is the assignment of *partial* or incomplete postcodes to addresses (e.g., SA2***).

4.3 Connecting computers

In surveillance, an important source of examples of identifiers is computer networks. An everyday process is *domain name resolution* in which various web and email addresses are mapped to a single common address. For example, in a bilingual country like Wales, domain names such as *swansea.ac.uk* and *abertawe.ac.uk* have equal status and are mapped to a standard address. In general, domain names are often bought along with abbreviations and related choices. So, the association of domain names to a site is many-one.

Single sign-on systems enable users to log into different accounts via a single account using just one identity. Commonly, single sign-on applies to accounts that belong to a single organisation or security domain. More generally, *federated identity* management links identities across two or more independent organisations or security domains. To be trustworthy, common policies, practices and tools for mapping identity data are used. Examples are services like *Shibboleth* that provide remote access to library services in universities or public service organizations[7] and *eduroam* that is used for access to services across international research and education networks.[8] These transformations create one-many associations.

When connecting a computer to the Internet, a number is needed called an IP address (32 bits under IP Protocol 4) that identifies the machine in the context of the service network (Layer 3).

[7] See: https://www.shibboleth.net

[8] See: https://www.eduroam.org

In some organisations there is a sufficient pool of IP addresses allocated that an IP address for each machine can be assigned that does not change; these are called static IP addresses, and the association of computers to IP addresses in the context of the organisation is one-one.

However, commonly (e.g., at home), IP addresses are generated by the internet service provider in response to a customer's need for Internet access. The IP address is assigned to the router and is the same for all devices connected to that router. Thus, IP addresses can change over a period and the association of computers to IP addresses is many-one. This technique, called *network address translation* (NAT), is essential given the limited size of the IP address space.[9] The distribution of identity information is also common and makes identity data more obscure and harder to track.

There are many other identifiers, such as the media access control (MAC) addresses and CPU ID. The MAC address is a permanent identifier for addressing the hardware of the network (Layer 2); the MAC address is not communicated outside the network. The assignment of MAC addresses to devices is one-one. In the UK it is a requirement for organisations to be able to identify users on their network. Uniquely identifying a computer throughout its life can be difficult.

5. The creation, provenance, comparison and transformation of identifiers

Creating identifiers is an everyday occurrence – we open accounts, register for services, and buy products. For many of these actions, we rely on a handful of pre-existing identifiers; indeed,

[9] It was foreseen in 1996 (see: *Request for Comments 1918* of the Internet Engineering Task Force (IETF)).

for many services an email address is sufficient. To buy a product, an address and a credit card account number are usually sufficient for the vendor, which of course depends on having a bank account. To open a bank account in the UK, we give proof of our identity and current address, e.g., by using a passport and a recent utility bill to show residence. At face value, the quality of a bank identifier is guaranteed by the databases of the state (passport) and commerce (utility provider). The passport provides a high-quality identifier based on a birth certificate, a photograph, witness testimony, and possibly other biometric data.

The quality of an identifier is essentially a matter of its reliability, which in turn depends on the process involved in creating it, i.e., its provenance. Examples demonstrate that *the creation of new identifiers depends on pre-existing identifiers*. The dependability of one identifier upon another can be illustrated pictorially by drawing a network of dependences which consist of nodes and links. The identifiers appear in the nodes and their dependency is marked by an arrow between nodes. In the case of high quality and trusted identifiers like the bank accounts, the graphs have a simple structure like a tree. The networks created we call *identity dependency graphs*; and the paths in these networks that trace dependences of one identifier on others we call *identity chains*.

The creation of stable trustworthy identifiers is not straightforward (e.g., there are many naturally emerging unconnected dependency graphs). Block chain technology is an extreme manifestation of this as it is a complex and energy hungry process for making even digital objects truly unique – not least for financial purposes as in currencies and non-fungible tokens.

If a country had a national register of citizens that enabled an identity card system, then one could relate all personal identifiers to that national identifier. For political, economic and cultural reasons the UK, for example, has failed (recently) to introduce such a system.[10] Personal identity combines names with addresses, dates of birth and all sorts of other information depending on a situation, such as the right to medical treatment, drive a car or to enter or reside in a country.[11]

5.1 Accounts - anonymous, hidden and revealed

Identity is essential to online accounts as usernames and passwords are required for access. In general, an account holder may have options in declaring his or her identity, and different ways of gaining access. Some accounts are *anonymous* as they can be set up without the provider having any information about the holder; examples include some free email and social media accounts (e.g., ProtonMail, Guerrilla Mail, Mailinator Mail, …, Twitter, Facebook, Plenty of Fish). By extension, anonymity can be preserved by free services that only ask an account holder for an email address.

Some accounts are *publicly hidden and privately revealed* as the account holder is invited to create a username and profile to be visible to others that may be fictitious, but the holder is required to provide personal data to the provider. If the provider needs payment then a bank

[10] An excellent summary is [60].

[11] A dramatic example is that of the Windrush generation, whose rights to employment, housing, medical care and mobility were questioned: http://www.bbc.co.uk/news/uk-43782241.

account must be declared, which means that the provider has a verifiable personal identifier for the account holder. Cybercommunities with subscription charges, like Second Life, are examples. Some accounts are *publicly revealed* as the holder often considers them to be about themselves, such as accounts for professional networking services, e.g., LinkedIn, and for socialising with friends like Facebook and Instagram.

5.2 Personal identity

The examples lead us to reflect on the data upon which we rely to distinguish a unique individual and guarantee his/her *embodied* identity; call them personal identifiers. In the UK, accuracy in personal identification commonly depend on passports [61], drivers licences (DVLA) and the National Identity Register (NIR) [62]. In criminal justice, where there is a need for the highest accuracy, identity depends upon on fingerprinting [63] and DNA samples [64]. Biometrics are expanding their scope of application [65]. Identifiers are assigned to the individual in pacific contexts. One fundamental problem for surveillance in which the entities are people is: How are identifiers able to actually identify a specific individual? One answer is that the person possesses identifiers that can be subjected to certain operations characteristic of the context. Among the operations are those we have called surveillance. Let us look at two examples of identifiers: (i) biometrics and (ii) social media.

Biometrics. Biometrics refers to the identification of humans by their physical characteristics or traits. Biometric identifiers are distinctive *measurements of* characteristics used to label and describe individuals; they begin with photography and finger printing. Operationally, the associations of biometrics to people are intended to be one-one. However, like all measurements, those used to test biometrics are approximate. Thus, it is a matter of high *probability* that biometric data manifests a one-one association of identifiers. The operational

tests invariably involve digital scanning. The identifiers generated by the scanners are mathematical approximations of physical features and can be proprietary, being implemented with different degrees of resolution by different manufacturers. Biometrics are fundamental in the development of information security [66].

Social media. To log into social networking site, an individual needs a unique user name and password combination. To sign-up for a new account on Facebook, for example, an individual must enter his/her name, birthday, gender and email address into an online form on its site and then to pick a password. Upon completing the sign-up form, an email is sent to the email address provided. The sign-up process is completed by clicking the confirmation link embedded in the email. This process is common.

The next stage is to create a basic profile to highlight some key characteristics of the individual. This could include basic information (birthday, relationship status, religious views), work and education, relationships and family, and contact information. An individual's 'user name & password' and 'basic personal profile' form his/her identifier (see: Figure 1), which of course can be fictitious. Interaction with other individuals is the point of having a social media account. Finally, 'interaction history' forms the last part of a typical social media account (recalling the third part of a typical customer account: 'account history'). In the case of Facebook, an individual's 'interaction history' covers all his/her activities on Facebook, which include updating his/her status; commenting on another's post, status or photo; and sending other users private messages. The behaviour is the interaction history, which can be reasonably termed a *persona* in some social contexts.

Finally, notice that, operationally, the owner of the account is the owner of the email address,

who can control access, e.g., by generating a new password when forgetting the old. This feature is wide-spread among Internet accounts of all kinds: it is an identifier transformation, reducing account identifiers to email addresses.

5.3 The entity-identifier gap

The association of identifiers to objects is rigorous and sound. Commonly, the output of a surveillance situation is information about the behaviours of entities that are digital devices, rather than the users or owners of digital devices. The surveillance of devices is direct whilst the surveillance of users of devices is indirect – the data is about the device. A second fundamental problem for surveillance systems in which the entities are people is: How can we bridge the *identity gap* between the identifiers of devices and the identifiers of users. In general, bridging the gap is a process of finding a personal identifier that corresponds with the device identifier. The personal identifier may well be the strong kind discussed in the sub-section on personal identity.

6. Conclusion

In this paper, we have identified and characterised in the desiderata, a theoretical gap in surveillance studies, and proposed an abstract conceptual framework to inform the study of surveillance and identity focussed by the technical nature of digital technologies.

Our concepts are independent of (i) application domains; and (ii) technologies that capture data about the behaviour of people and objects. Thus, in principle, they could be applied to situations in the past, present or future. As people use more and more software, surveillance will penetrate

deeper into our everyday life [67]. In more contexts their identities become more extended, varied and fragmented.

Our conceptual framework is based upon precisely defined surveillance contexts. The idea of the context with its four components is intended as a tool for the rigorous dissection of surveillance issues, helping precise specifications to be developed of what can and cannot – should or should not – be surveilled in a context. It also makes explicit how different contexts may or may not be combined and extended. The identity of people and objects in a context are defined by means of data that we call identifiers. Commonly, identifiers are dependent on other identifiers. The abstract notion of identifier enables us to make explicit some socio-technical properties of surveillance, such as the complexities of establishing personal identity even in simple scenarios.

Underlying surveillance are more general phenomena, such as *archiving* and *monitoring*. It is to be expected that theorising surveillance will lead us to discover new subtle concepts and classifications for such phenomena. Dodge and Kitchen's logjects draws attention to distinct notions of system logs, which create curated records that collect data of interest.

Our proposed framework can be used to distinguish the notion of monitoring from surveillance. The modern world's appetite for monitoring and identifying people, animals, objects and raw materials grows and grows with scientific advances. Technologies that provide rigorous identification methods for products are long established – the barcode originates in the 1960s [68]. In various industries, such as agriculture and manufacturing, it is possible to trace products through supply chains to the sources of raw materials. In the workplace, monitoring ranges from clocking in, through performance indicators and professional reviews, to real-time

holistic staff monitoring [69]. Historically, monitoring in the workplace is central to the scientific management movement of F W Taylor [70]. Actually, there new demands for monitoring data to create training sets for AI learning systems designed to automate decision making; this is motivating new areas of surveillance.

For some, the allegory of *The Prisoner* may still seem extreme, even in terms of surveillance. Nevertheless, today, it *seems* perfectly possible to turn the digital infrastructure of our society into a digital panopticon, wherein perfect surveillance is possible across *many* connected contexts, at least in principle [33]. The latest invasions of software – the internet of things, autonomous machines, cloud services, smart environments, wearables – enable such a digital panopticon to be imagined and become more accurate in its digital representation and approximation of the world. Issues large and small arise from these applications that require integrating technical knowledge of data with philosophical, social and political thinking.

Our desiderata and abstract definitions offer a conceptual structure to work within both the technical and the social. Indeed, the role of data, software and hardware in society means that social theories will become more and more amenable to mathematical analysis. Our definitions are sufficiently precise to allow us to formalise them in mathematical models using algebra and logic. As more and more of life is represented by and conducted through numbers such theories will become necessities.

Acknowledgements.

- Thanks to Imran Hussain and Gareth Ayres for useful discussions.

- This research was partially supported by the EPSRC project *Data Release - Trust, Identity, Privacy and Security* (EP/N028139/1, 2016-2020 and EP/N027825/1, 2016-2020).

References

[1] Lyon, D. (2001a). *Surveillance Society: Monitoring Everyday Life*. Open University Press.

[2] Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication & Society*, *5*(2): 242-257.

[3] Lyon, D. (ed.) (2003). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Routledge.

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

[5] Gandy, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press.

[6] Beck, U. (1986). *Risk Society: Towards a New Modernity*. Sage.

[7] Marx, G. T. (1989). *Undercover: Police Surveillance in America*. University of California Press.

[8] Ericson, R., & Haggerty, K. (1997). *Policing the Risk Society*. University of Toronto Press.

[9] Lyon, D. (2001b). Under my skin: from identification papers to body surveillance. In Caplan J. (ed.), *Documenting Individual Identity: the Development of State Practices in the Modern World*. Princeton University Press.

[10] Lyon, D. (2004). Identity cards: Social sorting by database. *OII Internet Issue Brief No3*.

[11] Lyon, D. (2007b). Surveillance, security and social sorting – Emerging research priorities, *International Criminal Justice Review*, *17*(3): 161-170.

[12] Bauman, Z., & Lyon, D. (2012). *Liquid Surveillance: A Conversation*. Polity Press.

[13] Brown, I. (2013). How will surveillance and privacy technologies impact on the psychological notions of identity? in *Future Identities: Changing identities in the UK – the next 10 years*. UK Foresight.

[14] Lianos, M. (2003) Social control after Foucault. *Surveillance and Society*, *1*(3): 412–430.

[15] Wills, D. (2013). *Surveillance and Identity: Discourse, Subjectivity and the State*. Ashgate.

[16] Ball, K., Haggerty, K. and Lyon, D. (ed.) (2012). *The Routledge Handbook of Surveillance Studies*. Routledge.

[17] Jenkins, R. (2004). *Social Identity*. Routledge.

[18] Fearon, J. D. (1999). What Is Identity (As We Now Use the Word)? Department of Political Science, Stanford University. Retrieved from http://www.web.stanford.edu/group/fearon-research/cgi-bin/wordpress/wp-content/uploads/2013/10/What-is-Identity-as-we-now-use-the-word-.pdf

[19] Wang, V., and Tucker, J.V., (2017). 'Surveillance and identity: Conceptual framework and formal models'. *Journal of Cybersecurity, 3*(3): 145–158.

[20] Crayford, M., & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying, *The Information Society*, 34(2): 88-103.

[21] Black, E. (2001). *IBM and the Holocaust*. Little, Brown & Company.

[22] Corera, G. (2016). *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage*. Pegasus Books (1778).

[23] Green, S. (1999). A plague on the panopticon: surveillance and power in the global information economy. *Information, Communication & Society*, *2*(1): 26-44.

[24] Linden, G., Smith B., & York J. (2003). Amazon.com Recommendations – Item-to-Item Collaborative Filtering. *IEEE Internet Computing* (January-February). Retrieved from https://www.cs.umd.edu/~samir/498/Amazon-Recommendations.pdf

[25] Smith, B., & Linden, G (2017). Two decades of recommender systems at Amazon.com, *IEEE Internet Computing*, *21*(3): 12-18.

[26] Langone, A. (2018, April 4). Facebook's Cambridge Analytica controversy could be big trouble for the social network. Here's what to know. *TIME (US)*. Retrieved from http://time.com/5205314/facebook-cambridge-analytica-breach/

[27] Kaspersky (2016, July 19). Stop iOS tracking. Kaspersky Lab. Retrieved from https://www.kaspersky.com/blog/ios-tracking-setup-part-1/12625/

[28] Dodge, M., & Kitchin, R. (2009). Software, objects, and home space. *Environment and Planning A*, 41(6): 1344 – 1365.

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

[30] Abel, A. (2018, January 18). Orwell's Big Brother' is already in millions of homes. Her name is Alexa. *Maclean's*. Retrieved from https://www.macleans.ca/society/technology/amazon-alexa-google-home-privacy-surveillance/

[31] Gray, A. (2018). *Here's the secret to how WeChat attracts 1 billion monthly users*. World Economic Forum. Retrieved from: https://www.weforum.org/agenda/2018/03/wechat-now-has-over-1-billion-monthly-users/

[32] Pham, S. (2018, March 1). China has found a new way to block banned words. *CNN tech*. Retrieved from https://money.cnn.com/2018/03/01/technology/china-wechat-censorship-ai/index.html

[33] Wang, V., Haines, K., & Tucker, J.V. (2011). Deviance and control in communities with perfect surveillance – the case of Second Life. *Surveillance and Society*, *9*(1/2): 31-46.

[34] Adams, A., & Ferryman, J. (2015). The future of video analytics for surveillance and its ethical implications. *Security Journal 28*(3): 272–289.

[35] Norris, C., & Armstrong, G. (1999). *The Maximum Surveillance Society: The Rise of CCTV*. Berg 3PL.

[36] Clarke, R. (1993). Computer matching and digital identity. Paper presented at *Computers, Freedom & Privacy*, (CFP'93), San Francisco. Retrieved from http://www.rogerclarke.com/DV/CFP93.html

[37] Clarke, R. (1994a). The digital persona and its application to data surveillance. *The Information Society*, *10*(2): 77-92.

[38] Clarke, R. (1994b). Human identification in information systems: Management challenges and public policy issues'. *Information Technology & People*, *7*(4): 6-37.

[39] Clarke, R. (1988). Information technology and dataveillance. *Communication of the ACM, 31*(5): 498-512.

[40] Clarke, R. (2014). Persona missing, feared drowned: the digital persona concept, two decades later. *Information Technology & People, 27*(2): 182-207.

[41] Orwell, G. (1949). *Nineteen Eighty-Four*. Secker & Warburg.

[42] Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Penguin.

[43] Giddens, A. (1991). *Modernity and Self-identity: Self and Society in the Late Modern Age*. Polity Press.

[44] Thomas, J. M., Brey, P., & Feenberg, A. (2004). *Modernity & Technology*. MIT Press.

[45] Lessig, L. (2006). *Code and Other Laws of Cyberspace, Version 2.0.* Basic Books.

[46] Castells, M. (2009). *The Rise of the Network Society*. Wiley-Blackwell, 2nd edition.

[47] Matthewman, S. (2011). *Technology & Social Theory*. Palgrave.

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

[49] Goold, B., & Neyland, D. (2015). *New Directions in Surveillance and Privacy*. Routledge.

[50] Brown, I. (2013). How will surveillance and privacy technologies impact on the psychological notions of identity? in *Future Identities: Changing identities in the UK – the next 10 years*. UK Foresight.

[51] Deleuze, G. (1986/1990/1992). Postscript on the societies of control. *October*, *59*: 3-7.

[52] Karnow, C. E. A. (1994). The encrypted self: fleshing out the rights of electronic personalities. *John Marshall Journal of Computer & Information Law*, *13*: 1-17.

[53] Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. MIT Press, Boston.

[54] Dodge, M., & Kitchin, R. (2005). Codes of life: identification codes and the machine-readable world. *Environment and planning D: Society and Space*, *23*: 851 – 881.

[55] Simon, B. (2005), The return of panopticism: supervision, subjection and the new surveillance. *Surveillance & Society*, *3*(1): 1-20.

[56] Wen, J., Ming, K., Wang, F., Huang, B., & Ma, J. (2009). Cyber-I: vision of the individual's counterpart on cyberspace. *Proceedings of 8th IEEE Intl Conf. on Dependable, Autonomic and Secure Computing*: 295-302.

[57] Ma, J., Wen, J., Huang, R., & Huang, B. (2011). Cyber-individual meets brain informatics. *IEEE Intelligent Systems*. Retrieved from http://cis.k.hosei.ac.jp/Bjianhua/mahome/CyberIndividual_Meets_Brain_Informatics.pdf

[58] Jenkins, R. (2004). *Social Identity*. Routledge.

[59] Curran, D. (2018, April 6). Are your phone camera and microphone spying on you? *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/apr/06/phone-camera-microphone-spying

[60] Beynon-Davies, P. J. (2011). The UK National Identity Card. *Information Technology Teaching Cases 1*: 12-21.

[61] Torpey, J. (2000). *The Invention of the Passport: Surveillance, Citizenship and State*. Cambridge University Press.

[62] UK Government (2006). *The Identity Card Act 2006: Elizabeth II. Chapter 11*, London: The Stationary Office.

[63] Cole, S. (2001). *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press.

[64] Wallace, H. (2006). The UK national DNA database – Balancing crime detection, human rights and privacy. *Science & Society*, *EMBO reports 7*: S26-S30.

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

[66] Wayman, J. L. (2007). The scientific development of biometrics over the last 40 years. *The History of Information Security: A Comprehensive Handbook*. Elsevier Science.

[67] Martinez-Bejar, R. & Brandle, G. (2018). Contemporary technology management practices for facilitating social regulation and surveillance, Technology in Society, 54: 139 - 148.

[68] Weightman, G. (2015, September 23). The history of the bar code. Retrieved from https://www.smithsonianmag.com/innovation/history-bar-code-180956704/

[69] Waber, B. (2013). *People Analytics*, FT Press.

[70] 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.