1. Surveillance Society: summary, history, definitions

1.1. We live in a surveillance society. It is pointless to talk about surveillance society in the future tense. In all the rich countries of the world everyday life is suffused with surveillance encounters, not merely from dawn to dusk but 24/7. Some encounters obtrude into the routine, like when we get a ticket for running a red light when no one was around but the camera. But the majority are now just part of the fabric of daily life. Unremarkable.

1.2. To think in terms of surveillance society is to choose an angle of vision, a way of seeing our contemporary world. It is to throw into sharp relief not only the daily encounters, but the massive surveillance systems that now underpin modern existence. It is not just that CCTV may capture our image several hundred times a day, that check-out clerks want to see our loyalty cards in the supermarket or that we need a coded access card to get into the office in the morning. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living.

1.3. Conventionally, to speak of surveillance society is to invoke something sinister, smacking of dictators and totalitarianism. We will come to Big Brother in a moment but the surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy. Surveillance may be viewed as progress towards efficient administration, in Max Weber's view, a benefit for the development of Western capitalism and the modern nation-state.[1]

1.4. Some forms of surveillance have always existed as people watch over each other for mutual care, for moral caution and to discover information covertly. However, from about 400 hundred years ago, 'rational' methods began to be applied to organizational practices, that steadily did away with the informal social networks and controls on which everyday business and governing previously relied. People's ordinary social ties were made irrelevant so that family connections and personal identities would not interfere with the smooth running of these new organizations. But the good news was that by this means citizens and eventually workers could expect that their rights would be respected because they were protected by accurate records as well as by law.

1.5. When the nation-state was in its heyday, and departments proliferated, after World War Two, systems started to creak and even crumble under pressure. But help was at hand in the shape of new computer systems that reduced labour intensivity and increased the reliability and volume of work that could be accomplished. In time, with new communications systems, now known together as 'information technology' (IT), bureaucratic administration could work not only between

departments of the same organisation, but between different organisations and, eventually, internationally. Something very similar is also true of businesses, first keeping records, then networking, and then going global, courtesy of IT. Yet even such 'joined-up' activities relate to technical and modern desires for efficiency, speed, control and coordination.

1.6. Impersonal and rule-centred practices spawned surveillance. Essential to bureaucracy is the oversight of subordinates and creation of records within the system. Business practices of double-entry book-keeping and of trying to cut costs and increase profit accelerated and reinforced such surveillance, which had an impact on working life and consumption. And the growth of military and police departments in the twentieth century, bolstered by rapidly developing new technologies, improved intelligence-gathering, identification and tracking techniques. But the main message is that surveillance grows as a part of just being modern.

2. What is wrong with a surveillance society?

2.1. Understanding surveillance society as a product of modernity helps us avoid two key traps: thinking of surveillance as a malign plot hatched by evil powers and thinking that surveillance is solely the product of new technologies (and of course the most paranoid see those two as one). But getting surveillance into proper perspective as the outcome of bureaucracy and the desire for efficiency, speed, control and coordination does not mean that all is well. All it means is that we have to be careful identifying the key issues and vigilant in calling attention to them.

2.2. Surveillance is two-sided, and its benefits must be acknowledged. Yet at the same time risks and dangers are always present in large-scale systems and of course power does corrupt or at least skews the vision of those who wield it.

2.3. Take risks and dangers first. These are something we have become more used to since the public realisation dawned in the later twentieth century that 'progress' is a mixed blessing. Every increase of 'goods' production, as Ulrich Beck pithily put it, also means a greater output of 'bads.'[2]

2.4. In addition to the environmental ones uppermost in Beck's mind, some of those 'bads' are social and political ones. Large-scale technological infrastructures are peculiarly prone to large-scale problems. And especially where computer systems are concerned, one inadvertent or ill-advised keystroke can easily cause havoc. Think of the release for 'research' purposes, of twenty million of ordinary peoples' online search queries from AOL in August 2006. Supposedly shorn of identifiers, it took only moments to start connecting search records with names.[3] This report looks at some problems of large-scale surveillance systems.

2.5. It is equally important to remember the point about the corruptions and skewed visions of power. Again, we do not have to imagine some wicked tryant getting access keys to social security or medical databases to see the problem. The corruptions of power include leaders who appeal to some supposed greater good (like victory in war) to justify unusual or extraordinary tactics.

2.6. In the USA, Japanese Americans were singled out for internment during World War Two through the – normally illegal – use of census data. More recently, many Muslim Americans are branded as unfit for travel using no-fly lists or are otherwise subject to racial profiling, condemned in other contexts for its manifest unfairness.[4] Where white Americans may be able to circumvent airport delays by making slight changes to their names when reserving their flights, this is much harder for people whose names seem 'Arab' or 'Muslim'.[5] Any 'exceptional circumstances,' especially when the exceptions seem permanent as in an endless 'war on terror' are ones that require special vigilance from those who care about human and civil rights.

2.7. Beyond this, in the world of high technology and global commerce unintended consequences of well-meaning actions and policies abound. For example, in order to remain competitive, corporations, we are told 'know their customers' and thus pitch their advertising and even locate their plants and stores appropriately. No one suggests that the store manager wishing to lure only the most creditworthy customers is devious in obtaining credit check services from various credit referencing agencies. It simply makes sense in the quest for greater profitability. But the results – the unintended consequences – of sifting through records to create a profitable clientele is that certain groups obtain special treatment, based on ability to pay, and others fall by the wayside.[6]

2.8. Three other points should be made about 'what's wrong with surveillance society.

2.8.1. The first follows from what was said about exceptional circumstances and unintended consequences. It is imperative to scrutinize systems that permit gross inequalities of access and opportunity to develop. Of course, as all true surveillance systems are meant to discriminate between one group and another, this is difficult, but the problem can at least be brought into the open. Unfortunately, the dominant modes of surveillance expansion in the twenty-first century are producing situations where distinctions of class, race, gender, geography and citizenship are currently being exacerbated and institutionalized. Our report details these.

2.8.2. Secondly, and for social cohesion and solidarity most profoundly, all of today's surveillance processes and practices bespeak a world where we know we're not really trusted. Surveillance fosters suspicion.[7] The employer who installs keystroke monitors at workstations, or GPS devices in service vehicles is saying that they do not trust their employees. The welfare benefits administrator who seeks evidence of double-dipping or solicits tip-offs on a possible 'spouse-in-the-house' is saying they do not trust their clients. And when parents start to use webcams and GPS systems to check on their teenagers' activities, they are saying they don't trust them either. Some of this, you object, may seem like simple prudence. But how far can this go? Social relationships depend on trust and permitting ourselves to undermine it in this way seems like slow social suicide.

2.8.3. The final question for surveillance society has to do with a nagging worry that surveillance, especially that associated with high technology and anti-terrorism, distracts from alternatives and from larger and more urgent questions. We may ask whether this is really the best way of pursuing these goals. Unfortunately, and without succumbing to cynicism, we have to note that procuring new technology surveillance supports the economy, helps to keep out 'undesirables,' yields the appearance of definite action, gives the impression that the exits are sealed and supports a business-as-usual attitude.

3. Defining surveillance; tracing surveillance society

3.1. Definitions are vital, especially with a controversial word like surveillance. Often thought of in rather specific, targeted terms, in reality it is much more. Rather than starting with what intelligence services or police may define as surveillance it is best to begin with a set of activities that have a similar characteristic and work out from there. Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance.

3.2. To break this down:

- The attention is first *purposeful*; the watching has a point that can be justified, in terms of control, entitlement, or some other publicly agreed goal.
- Then it is *routine*; it happens as we all go about our daily business, it's in the weave of life.
- But surveillance is also *systematic*; it is planned and carried out according to a schedule that is rational, not merely random.
- Lastly, it is *focused*; surveillance gets down to details. While some surveillance depends on aggregate data, much refers to identifiable persons, whose data are collected, stored, transmitted, retrieved, compared, mined and traded.

3.3. The personal details in question may be of many kinds, including CCTV images, biometrics such as fingerprints or iris scans, communication records or the actual content of calls, or most commonly, numerical or categorical data. Because so many data are of the last type referring to transactions, exchanges, statuses, accounts and so on, Roger Clarke has called this 'dataveillance.'[8] Dataveillance monitors or checks people's activities or communications in automated ways, using information technologies. It is far cheaper than direct or specific electronic surveillance and thus offers benefits that may sometimes act as incentives to extend the system even though the data are not strictly required for the original purpose.

3.4. Most surveillance today is of the kind just described – though it must not be forgotten that face-to-face human surveillance is far from extinct – and is carried out overwhelmingly by large organizations that have an interest in one of the goals mentioned. But the falling costs of surveillance equipment also induces others to engage in automated activities that include watching, observing, and even snooping and voyeurism. Some peer-to-peer surveillance occurs as when spouses use cellphones to find out about each others' activities (and again, trust has eroded in

such cases), and watching from below – or 'sousveillance' – may also occur when ordinary people grasp the cameras and watch the watchers.[9]

3.5. What, then, of surveillance as an adjective, to describe a kind of society? Where did the idea of surveillance society come from? Not surprisingly, it started cropping up after the first wave of computerization of organizations in the 1970s. At that time, the key metaphor was 'Big Brother' from George Orwell's famous novel *Nineteen-Eighty-Four*. By the 1980s a number of serious studies was building on those of the 1970s[10] and some started to use the term 'surveillance society.' Gary T. Marx invoked *Nineteen-Eighty-Four* in what was the first social science reference to computer-based 'surveillance society' in 1985 and this was followed by Oscar Gandy's comments on 'bureaucratic social control' – a reference to Max Weber's work, also updated for digital times, that also warned about 'surveillance society'.[11]

3.6. Interestingly, our image of state surveillance is often shaped by novels and films. Prominent examples are Franz Kafka's *The Trial* (1914), in which the enigmatic figure of Josef K (what happened to his name?) confronts unknown accusers on unclear charges, or George Orwell's *Nineteen-Eighty-Four* (1948) that paints a terrifying picture of detailed, damning surveillance by the nation-state, personified by the sinister, looming figure of 'Big Brother'. These highlight the crucial role of information (or lack of it, for the surveilled) within bureaucratic governments, alongside the constant threat of totalitarianism.

3.7. What neither Kafka nor Orwell could have foreseen was the rise of computers and the wholesale digitizing of administration. After all, the 'silicon chip' did not appear for another thirty years after *Nineteen-Eighty-Four*. From the 1970s, however, computers were to make for a massive expansion in the ways in which surveillance and bureaucratic control occurred. While the dilemmas of surveillance are brilliantly explored in *The Conversation* (1974) this movie relies primarily on conventional audio-surveillance and eavesdropping. More recent films such as *The Net* (1995), *Enemy of the State* (1998), and *Minority Report* (2002) deal more directly with IT-based surveillance. However, movies, being sensational, depend on their success on exploiting technological capabilities, rather than on the actual everyday consequences of living in surveillance societies.

3.8. This is why returning to the social sciences is helpful. Whatever changes have taken place in business and government since Weber's time – computerization, networking, globalization and even 'relationship management' – the underlying principles still stand. This is why Weber's views on the modern world of surveillance are so telling. He saw this surveillance, keeping detailed records, collating information, limiting access to certain eligible persons, not as mere evidence of 'progress,' but as deeply ambiguous. At worst, he predicted that the efficient but soulless world of bureaucratic organization would become an 'iron cage.' Ordinary people would feel trapped in an impersonal, uncaring system. Add the malicious indifference of Josef K's interrogators or the whims of a ruthless dictator like 'Big Brother' and you have a recipe for repression as well.

3.9. But we also have to go beyond Weber, because not only is surveillance society today highly technological, it has long ago spilled over the edges of the state and into corporations, communications and even entertainment (indeed, *Big Brother* a TV series shows how surveillance is domesticated and becomes participatory in new ways[12]). Surveillance is bound up with what we call 'governance.' This goes far beyond what governments do; the 'computer state' is now a dated idea. Governance refers to how society is ordered and regulated in manifold ways. Governance controls access, opportunities, chances and even helps to channel choices, often using personal data to determine who gets what. Actuarial practices all-too-often take over from ethical principles.

4. Perspectives on the Surveillance Society 1: Issues

4.1. We turn now to an inventory of issues and processes that relate to the surveillance society as it has just been outlined. This is intended as a catalogue or check-list of important things to consider when discussing the surveillance society. It is important to note that although these vary in time and place in some form they are crucially significant for understanding the basic contours of surveillance society.

4.2. *Privacy, ethics, human rights.*

4.2.1. Since the 1970s, much reflection and legal discussion of surveillance has occurred, producing data protection laws in Europe and privacy law elsewhere. Such regulation adopts a specific understanding of privacy. Although the 'Fair Information Principles' (FIPs)[13] that have evolved and have received widespread assent work from a basic understanding of the importance of privacy to individual citizens, it has proved difficult to persuade policy-makers of the salience of the *social* dimensions of privacy[14] let alone of the need to confront problems associated with the surveillance society as such. It is also the case that to jolt a legal process into action, the individual has to know something's wrong, identify what it is and know where to take the complaint and how to find redress.

4.2.2. Surveillance society poses ethical and human rights dilemmas that transcend the realm of privacy. Without minimizing the human and democratic need for privacy, and acknowledging that if only large organizations complied fully with data protection and privacy legislation many surveillance society problems would be reduced, we insist that those problems deserve to be approached in other ways. Ordinary subjects of surveillance, however knowledgeable, should not be merely expected to have to protect themselves. Three key issues are as follows:

4.3. *Social exclusion, discrimination.*

4.3.1. As we show in this report, surveillance varies in intensity both geographically and in relation to social class, ethnicity and gender. Surveillance, privacy-invasion and privacy-protection differentiate between groups, advantaging some and, by the same token, disadvantaging others. It is not because of surveillance, of course, that the nation-state today feels it can no longer offer the kinds of social security that it once aspired to, or that it now

downscales its aims to providing only some forms of basic individual safety.[15] Rather, surveillance grows alongside these changes, usually supporting or at least enabling them. As well, the agencies of individual safety can easily be outsourced.

4.3.2. Cradle-to-grave health-and-welfare, once the proud promise of social-democratic governments, has been whittled down to risk management and – here's where the surveillance society comes in – such risk management demands full knowledge of the situation. So personal data are sought in order to know where to direct resources.[16] And because surveillance networks permit so much joining-up, insurance companies can work with police, or supermarkets can combine forces with other data-gatherers so much more easily. The results, as we shall see, are that all-too-often police hot-spots are predominantly in non-white areas, and supermarkets are located in upscale neighbourhoods easily reached by those with cars.

4.4. *Choice, power and empowerment***.**

4.4.1. So what say do ordinary citizens, consumers, workers and travelers have in shaping the surveillance society? It must be again stressed that the surveillance society is not a conspiracy, and neither are the outcomes technologically determined. Ordinary people can and do make a difference especially when they insist that rules and laws be observed, question the system or refuse to have their data used for purposes for which they have insufficient information or about which they harbour doubts.

4.4.2. But how far can individuals and groups choose their exposure to surveillance and limit personal information collected and used? When the surveillance system is infrastructural, and when its workings are shrouded in technical mystique, it is very hard indeed to make a significant difference. For instance, not until some identity theft scandal breaks do consumers become aware of the extent of personal profiling carried out by major corporations.[17] Even then, the focus tends to be on security – how to prevent similar fraud – rather than on curbing the power of businesses and state agencies promiscuously and prodigiously to process so much data. Although as we argue later, individuals are not alone in surveillance regulation, which may depend heavily on specialised agencies and commissions in countries with data protection or privacy law, as well as on professional and other associations, these mechanisms are not necessarily effective. Individuals are seriously at a disadvantage in controlling the effects of surveillance.

4.5. *Transparency, accountability***.**

4.5.1. Business, transport and government infrastructures all have mushrooming surveillance capacities but individuals and groups find it difficult to discover what happens to their personal information, who handles it, when and for what purpose. Indeed, most of the time, ordinary citizens and consumers simply do not have the time or the incentive to go in search of such details. Yet little by little, their personal data are used to help shape their life chances, to guide their choices. Given the power of large organisations with sophisticated surveillance capacities, however, it seems only fair that ordinary people should have a say,

even if only at the level of principle. This may be sought, not only through specialized agencies but also through advocacy groups and the mass media.

4.5.2. Accountability should be assumed within organizations, especially when high-powered surveillance occurs routinely, with potentially damaging consequences. Although workplace surveillance offers some salutary examples of poor practices, as we shall show, at least in some instances employers have been obliged to curb the excesses of their monitoring by active labour union intervention. And as examples in this area show, much can be achieved through a transparent process of employers explaining what the monitoring entails and negotiating acceptance for it from employees. When it comes to consumer surveillance, however, no analogue exists, and yet the massive data-power of a Tesco or a Walmart is almost unparalleled. The emergence of today's surveillance society demands that we shift from self-protection of privacy to the accountability of data-handlers. Such work parallels the efforts of regulators to enforce controls and to press for the minimising of surveillance.

5. Perspectives on the Surveillance Society 2: Processes

5.1. *Social sorting*.

5.1.1. In the surveillance society, social sorting is endemic. In government and commerce large personal information databases are analysed and categorized to define target markets and risky populations.[18] In the section on consumer surveillance we shall see how a company like *Amazon.com* uses sophisticated data mining techniques to profile customers, using both obvious and non-obvious relationships between data. This enables them to show who is most likely to buy what but also which customers are likely to be credit risks. As far as *Amazon.com* is concerned, you are their profile. *Amazon.com* benefits and no doubt some customers feel they do too. It saves searching time to be recommended other items. But there could also be negative consequences of customers. Once classified, it is difficult to break out of the box. Such non-obvious relationships are also sought when sorting out groups who wish to travel by airplane. Since 9/11 such sorting might possibly have contributed to safety in the air (we shall never know) but it has certainly led to crude profiling of groups, especially Muslims, that has produced inconvenience, hardship and even torture.

5.1.2. Social sorting increasingly defines surveillance society. It affords different opportunities to different groups and often amounts to subtle and sometimes unintended ways of ordering societies, making policy without democratic debate. As the section on urban infrastructure shows, invisible, taken-for-granted systems of congestion charging and intelligent public transit both sort the city into groups that can travel relatively freely and others who find travel difficult and at the same time can be used for crime control and national security. No one has voted for such systems. They come about through processes of joined-up government, utility and services outsourcing, pressure from technology corporations and the ascendancy of actuarial practices.

5.2. *Data flow*.

5.2.1. Data gathered by surveillance technologies flow around computer networks. Many may consent to giving data in one setting, but what happens if those data are then transferred elsewhere? In order to protect children from abuse, or to reduce fraud in public services, frequent calls are made to draw on more and more varied databases. Yet there is already all-too-little knowledge either among the public or among data-sharing agencies about where exactly those data travel. The idea that policy interventions be 'intelligence-led' has taken hold and this, along with the networking and data-matching potentials of today's digital infrastructures, means that surveillance appears to operate by a logic of its own.

5.2.2. But that logic needs to be questioned, examined and checked, particularly in regard to processes that involve data-flow from one setting to another. Such data flows require description and analysis. While one major question is, how secure are databases from unauthorized access or leakage?, a further and more vital one is, to what extent should data be permitted to move from one sphere to another? It is a basic issue of FIPs, but one that invites a new urgency as the integration and harmonisation of 'intelligence-led' systems seems to be both technologically and administratively desirable.

5.3. *Function Creep*

5.3.1. The third process highlighted here is one that has already been mentioned in this introduction. Personal data, collected and used for one purpose and to fulfil one function, often migrate to other ones that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable. In the case of Oyster cards in the UK, data that begin life in the commercial sphere of public transit, are increasingly required in police inquiries.[19] Such data may also stay in the same context but as their uses grow, they may acquire some dangerous characteristics. Medical surveillance, as we shall see, is a case in point. Diagnostic technologies that may have some utility in individual cases may gradually be allowed to creep towards broader and broader contexts, weakening their predictive qualities for positive diagnosis along the way. Those falsely diagnosed may well be disadvantaged.

5.3.2. Function creep usually happens quietly, unobstrusively, as a bit of administrative convenience. But it profoundly challenges FIPs and, despite the fact that it was identified as a problem several decades ago, is still a major issue. Indeed, because new technologies permit increasing amounts of data interchange and because organisational efficiency is frequently seen as a top priority, the human consequences of function creep are all-too-often unknown, ignored or downplayed.

5.4. *Technologies***.**

5.4.1. Surveillance today is often thought of only in technological terms. Technologies are indeed crucially important, but two important things must also be remembered: One, 'human surveillance' of a direct kind, unmediated by technology, still occurs and is often yoked with more technological kinds. Two, technological systems themselves are neither the cause nor the sum of what surveillance is today. We cannot simply read surveillance consequences off the

capacities of each new system (especially if those capacities are described by the vendor). But if technologies are indeed important for surveillance, how should they be viewed?

5.4.2. For the surveillance society properly to be understood, technologies should be analysed and monitored in an ongoing way. We have to understand how they work (what the software and hardware does), how they are used (this is an interactive process, involving in-house personnel as well as technology consultants and operatives), and how they influence the working of the organisation. Moreover, we need to understand these things clearly enough to influence policy and practice as our later discussion of impact assessments suggests.

5.4.3. Similar technologies are used today in different settings, encouraging the development of joined-up surveillance. Recent developments, such as location technologies, permit geographical tracking of persons and goods in real time and current developments such as ambient intelligence, with embedded, wearable and implanted devices take this even further. One important implication is that those with ethical insights gleaned from the critical analysis of surveillance society should be involved at every stage of implementation. Systems become much less amenable to change after they have been established.

5.4.4. A third concern regard technologies is that many argue (mistakenly, as we shall see) that anxieties about surveillance society may be allayed by technical means. Certainly, some so-called privacy-enhancing technologies serve well to curb the growth of technological surveillance (PETs) and their use should be encouraged where appropriate. But these are at best only ever part of the answer. We are correct to be wary of any offers to fix what are taken to be technical problems with technical solutions. As we shall see, the real world of surveillance society is far to complex for such superficial responses.

6. A Guide to the Report

6.1. Following this Introduction (Part A), this Report has several further parts:

- Part B distils the findings of nine separate specially commissioned expert reports into a wide-ranging survey of the Surveillance Society.
- Part C illustrates the Surveillance Society, through a scenario, a week in the life of an imaginary family in 2006; and secondly, through a series of glimpses of how some of the encounters and experiences of this family might play out in ten years time, in the year 2016.
- Part D concerns what regulators (both government and ‘watchdogs’ like the Information Commissioner) can do to curb the worst aspects of surveillance.
- Part E provides suggestions of Further Reading.
- All the expert reports are provided in full as appendices.

6.2. Accompanying the full report is a Public Discussion Document, designed to provoke discussion and debate amongst the public at large.