A Report on the Surveillance Society

For the Information Commissioner by the Surveillance Studies Network

September 2006

Full Report

Credits

Editor:

David Murakami Wood

Report Authors:

Kirstie Ball
David Lyon
David Murakami Wood
Clive Norris
Charles Raab

Expert Reports:

Louise Amoore
Kirstie Ball
Stephen Graham
Nicola Green
David Lyon
Jason Pridmore
Clive Norris
Charles Raab
Ann Rudinow Saetnan

Critical Readers:

Sarah Earle
Graham Sewell

Additional Material:

Emily Smith

Administrative Support

Anne Fry

Business Development:

Mark Siddoway / Knowledge House

Index

Part A: Introducing the Surveillance Society

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

[1] Gerth, H. and Wright Mills, C. (1964) *From Max Weber*, New York: .

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] Beck, U. (1992) *The Risk Society*, Newbury Park CA: Sage.
[3] See: Barbaro, A. and Zeller, T. 'A face is exposed for AOL searcher no. 4417749', *New York Times*, 9 August 2006. http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/

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.

[4] See: Amnesty International USA (2004) *Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA*, New York: Amnesty International USA, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf
[5] Kehaulani Goo, S., 'Hundreds Report Watch-List Trials' 21 August 2004, http://www.washingtonpost.com/ac2/wp-dyn/A20199-2004Aug20?language=printer
[6] Lace, S (2005) *The Glass Consumer*, Bristol UK: Policy Press; Danna, A. and Gandy, O. (2002) 'All that glitters is not gold: Digging beneath the surface of data-mining' *Journal of Business Ethics*, 40: 373-386; Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York: Routledge.
[7] This is discussed in: Lyon, D. (2003) *Surveillance after September 11*, Cambridge UK: Polity Press, 45-48, 142ff.

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

[8] Clarke, R. (2006[1997]) 'Introduction to dataveillance and information privacy', http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV

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.

[9] Mann, S., Nolan, M and Wellman, B. (2003) 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & Society* 1(3): 331-355.
[10] Such as: Rule, J. (1973) *Private Lives, Public Surveillance*, London: Allen Lane. The best-known in the 1980s were probably: Burnham, D. (1983) *The Rise of the Computer State*, New York: Vintage Books; and Marx, G.T. (1988) *Undercover: Police Surveillance in America*, Berkeley: University of California Press.
[11] Marx, G.T. (1985) 'The surveillance society: the threat of 1984-style techniques' *The Futurist*, June: 21-26; Gandy, O. (1989) 'The surveillance society: information technology and bureaucratic social control' *Journal of Communication*, 39:3.

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

[12] See: McGrath, J. (2004) *Loving Big Brother*, London: Routledge; Andrejevic, M. (2004) *Reality TV: The Work of Watching*, Lanham MD: Rowman and Littlefield.
[13] FIPs are the North American equivalent of European 'data protection principles.'
[14] See the excellent treatment of the sociality of privacy in: Regan, P. (1005) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press.

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,

[15] See e.g.: the discussion in: Bauman, Z. (2006) *Liquid Fear*, Cambridge UK: Polity Press.
[16] Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
[17] See the *New York Times* editorial, 'The data-fleecing of America' June 21, 2005.

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*.

[18] See the classic study: Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.

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

[19] See: 'Oyster data use rises in crime clamp-down' *The Guardian*, 13 March 2006, http://politics.guardian.co.uk/foi/story/0,,1730771,00.html

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.

Part B: A Survey of the Surveillance Society

7. Introduction

7.1. The Surveillance Studies Network commissioned a number of expert reports which are appended. These reports covered: Health and Medicine; Consumption; Work and Employment; Public Services; Citizenship; Crime and Justice; Communications; Built Environment and Infrastructure; and, Borders. From these reports, several key themes emerged which can be grouped into four areas: the context of the surveillance society; surveillance technologies; the processes by which surveillance operates and is implemented; and finally, how surveillance impacts on individuals and groups in society. There is of course, a great deal of overlap between these areas, and even more that could not be included.

8. The Context of the Surveillance Society

8.1. We first outline several underlying trends in western societies that lead to the surveillance society. These are: risk and security; the role of the military; the political economy of surveillance; and finally, the growing personal information economy.

8.2. *Risk and Security*

8.2.1. We live in a society obsessed by risk. Risk management techniques dealing with external threats have become a key part of organisational activities, which has intensified with the 'war on terror.' Internal risk assessment procedures are also more and more common. Of course, post 9/11 risk management is not entirely new and there is ample historical evidence of risk profiling prior to 9/11.[20]

8.2.2. However, a *pre-emptive* as opposed to a *preventative* approach to risk has emerged.[21] Current and emerging practices feature technologies and data-mining to this end. Significantly, pre-emptive risk profiling shifts surveillance practices toward the screening of the actions and transactions of the general population.[22] This screening can then be used to target interventions on people or groups of people who are considered to be at risk or to pose risks for others. Hence collection and analysis of information, including data on identifiable individuals are vital.

[20] Bigo, D. (2002) 'Security and immigration: toward a critique of the governmentality of unease', *Alternatives* (27): 63-92; Andreas, P. and Snyder, T. (eds.) (2000) *The Wall Around the West: State Borders and Immigration Controls in North America and Europe*, Lanham MD: Rowman and Littlefield.
[21] Ewald, F. (2002) 'The return of Descartes' malicious demon: an outline of a philosophy of precaution', in Baker, T. and Simon, J. (eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.
[22] Valverde, M. and Mopas, M. (2004) 'Insecurity and the Dream of Targeted Governance', in Larner, W. and Walters, W. (eds) *Global Governmentality: Governing International Spaces*, London: Routledge.

8.2.3. Surveillance is such a key component of living with risk that it might even be more appropriate to call the surveillance society, the 'risk-surveillance society'. The response to risk is an emphasis on safety and security. The 'risk-surveillance society' has allowed the emergence of a 'safety state' obsessed with security and stability. 'Better safe than sorry' stands as a motto that supports the considerable rise in social-care referrals for child abuse, and that gives a green light to the precautionary surveillance of groups, categories and individuals by the public services. This can confer personal and social benefits, but at the same time the conception of safety and security has important implications for liberty, privacy and other social values, as well as for innovation and change, which are inherently risky.

8.2.4. Several examples can illustrate this trend to risk assessment and pre-emption: the first is the rise of epidemiology and modelling within medical surveillance[23]. Medical surveillance for public health purposes takes three main forms, firstly monitoring and tracking individual disease cases. This occurs not just for the patient's own risk but also to identify sources of infection and/or genetic risk, to identify and alert potentially infected individuals who have been in contact with a person carrying an infectious disease (like AIDS or TB) or affected relatives bearing the same genetic risk (e.g.: Huntingdon's Chorea). Secondly, recording occurrences of disease for statistical analysis (e.g. identifying cancer clusters by analysing data in a cancer register). Third, screening whole populations to identify individuals or groups at higher than average risk for a disease (e.g. mass screenings for high blood pressure, or routine mammographies for early identification of breast cancer). Genetics has attracted intense debate and commentary and it is increasingly the case that larger and larger databases of genetic information are being established both for health, criminal justice and commercial reasons.

8.2.5. Second one can see a wide variety of public policy areas.[24] Risk-based approaches, based on assessments of individuals, families and neighbourhoods, are found in child protection and mental health, as well as in the criminal justice field of public protection. Neighbourhood statistics' responded to the need for better data for intelligence-led, tailored and targeted interventions co-ordinated across several agencies.[25] Some comprehensive programmes, for example the SureStart 'early years' programme for children, make intensive use of data about individuals. It also supports efforts to combat social exclusion and to deal with young offenders, and, especially, interventions in the education sector, new departures such as the children's database.

8.2.6. In criminal justice, risk has become paramount and underpinning the current focus of police and Home Office strategies is a consistent commitment to utilise surveillance strategies and technologies in an effort not only to drive down crime generally but, specifically to identify those at risk of criminal

[23] On the rise to power of health economics, a field that extensively applies techniques and results from epidemiology to the assessment of medical technologies, see e.g.: Ashmore, M., Mulkay, M.J. and Pinch, T.J. (1989) *Health and Efficiency: A Sociology of Health Economics*, Buckingham: Open University Press.

[24] 6, P., Raab, C. and Bellamy, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I'. *Public Administration* 83 (1): 111-133; Bellamy, C., 6, P., and Raab, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II'. *Public Administration* 83 (2): 393-415.

[25] Social Exclusion Unit, Cabinet Office (2000) *Report of Policy Action Team 18 on Better Information*. London: Social Exclusion Unit, Cabinet Office; Department for Work and Pensions (2001) *United Kingdom National Action Plan on Social Exclusion 2001-03*. London: Department for Work and Pensions.

behaviour; to focus proactively on the 'hardcore' of persistent offenders that the Government believes is most responsible for the crime problem[26].

8.2.7. From the protection of land borders to the policing of cross-border financial flows, from airport security to the screening of containers at sea ports, risk assessment has become the defining feature of border surveillance. Contemporary border surveillance involves the compilation, classification and categorisation of data on, for example passenger manifests or financial transactions, on an unprecedented scale. The USVISIT[27] border control system for a UK citizen crossing the US border mines some 30 databases, from previous entry and exit data to social security records and information on exchange students.

8.2.8. Using detailed personal and medical information in risk assessment is also of interest to both employers and the financial services industry. Although it is not current practice, the potential combination of consumer and medical information for credit referencing and insurance purposes raises major concerns over data accuracy, data use and fraud. Increasing both the quantity and quality of these data is a means for combating these issues, but this, in itself, has unsavoury consequences. Depending on how this information is used, the opportunities and life chances afforded to those who utilize and/or rely heavily on social services could be curtailed because they would be identified as 'high risk'. This is also applies to entire populations in particular areas, through the use of geodemographic data, which, in the context of consumer surveillance, can identify and assign relative risk to entire streets, postal codes or wider areas. The risk of investment is therefore passed from the organisation to its potential customers or users (and their geographic location), though there is little indication as to the means by which consumers and their neighbourhoods increase or decrease as a cost intensive risk.

8.2.9. Finally, in the workplace, personal medical information and biometrics are now seen by employers both as ways in which the identity of employees can be authenticated, and as a way of managing health and safety. For example, following widespread adoption in the USA, drug and alcohol testing is growing in the UK and is used especially where employees are in safety-critical jobs (e.g.: driving vehicles).

8.3. *The Militarization of Surveillance*

8.3.1. The drive to security is at least partly evidence of the continuing or revived importance of the military in western societies. Military surveillance is one of the few phenomena that can be said to be truly global in an age where everything is supposedly being globalized. The Earth is increasingly surrounded by a multitude of military surveillance satellites.

8.3.2. In addition transnational communications systems are thoroughly interpenetrated and infiltrated by military surveillance systems: even their invention, design and protocols have military elements. One example is the Global Positioning System (GPS), which was developed and is still ultimately controlled by the US military, which can alter its functionality in certain places and times when it suits military objectives. Another is the Internet. This

[26] Home Office (2001a) *Criminal Justice: The Way Ahead*, Cm 5074, London: Home Office, 20-23; but for a critique of the policy see: Garside, R. (2004) *Crime, Persistent Offenders and the Justice* Gap, London: Crime and Society Foundation.
[27] United States Visitor and Immigrant Status Indicator Technology, in place at all land, air and sea ports of entry from 2004.

transnational system of network connections and protocols was in no small part based on the American military's ARPANET distributed communications system, designed to survive destruction of particular parts of the system[28]. Indeed the entire history of modern surveillance can be traced from early development based in WW2 and Cold War Command Communications, Control and Intelligence (C3I) systems, with the aim being to make the planet a 'closed world', a totally defensible and secure space[29].

8.3.3. The development of surveillance technologies and processes result from a complex interaction between military and economic logics. Military organisations and methods of control have always been central in the development of the modern state. It was the control of military resources and the resting of the legitimate right to use force with institutions of the state which underlay the establishment of modern nation-states. This interaction manifests itself not only in the government and technological components, but also in the increasingly military way of talking about everyday safety: state and mass media talk of 'threat assessment', the 'war on drugs', the 'war on crime', and indeed 'the war on terror', of toughness in the law, of 'zero tolerance', and so on. The concepts of defensibility and gating have become mainstream parts of urban design. 'Information warfare' has come out of the dark shadows of military covert operations and into the bright light of the business world, where corporate espionage is rife and the computer penetration and security specialists are redesignated as 'knowledge warriors'.

8.3.4. However there are many concrete examples if one examines the history of technologies: many surveillance technology companies are intimately bound up with the military yet sell increasingly to civilian users. There is evidence of a shift of military supply and arms companies towards exploiting the civilian market, and indeed of creating new markets for innovative products that are no-longer purely military of civilian[30]. Major arms manufacturers have shifted into mainstream security and surveillance products: a good example is the progress of TRW, a major partner of the US defence contractor, which became a leader in civilian biometrics; in the UK, QinetiQ, the semi-privatised company formerly known as the Defence Evaluation and Research Agency (DERA); Sagem, in France, manufacturers of everything from mobile phones through surveillance algorithms to unmanned aerial reconnaissance systems; and so on.

8.3.5. In the 1990s, many argued that evidence of arms manufacturers shifting into civilian production represented a positive trend, part of a post-Cold War 'peace dividend', the social benefits that would supposedly flow from the end of the Soviet Union. But manufacturers who previously specialised in military contracting have moved into civilian production without abandoning their military roots, and have been quick to move back into military applications with the 'war on terror' along with many newer security companies specializing in particular surveillance technologies.

[28] Rheingold, H. (1994) *The Virtual Community*, London: Secker and Warburg.
[29] de Landa, M. (1991) *War in the Age of Intelligent Machines*, Cambridge MA: MIT Press; Edwards, P. (1997) *Computers and the Politics of Discourse in Cold War America*, Cambridge MA: MIT Press.
[30] Wright, S. (1998) *An Appraisal of the Technologies of Political Control: Interim STOA Report (PE 166.499)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme; Doucet, I. and R. Lloyd (eds.) (2001) *Alternative Anti-Personnel Mines: The Next Generation*, London / Berlin: Landmine Action / German Initiative to Ban Landmines.

8.4. *The Political Economy of Surveillance*

8.4.1. These new companies along with traditional security providers and the large military suppliers form part of what might broadly be called 'the security industry'. Other industrial sectors are also key to the growth of surveillance, in particular, telecommunications and computing and banking and insurance.

8.4.2. The security industry has grown massively in recent years. There are multiple ways of measuring this growth. For example, US consultancy Security Stock Watch's 100 company index of the security industry includes 'biodefense', 'environmental security', 'fraud prevention', 'military defense', telecommunications 'network security' and 'physical security' (barriers, video surveillance etc.). According to the index, the growth of the industry as a whole has consistently outperformed both the Dow Jones and the high-technology NASDAQ indices[31]. At the end of the financial year 2005-6, the index had more than doubled in 3 years, with an estimated market capitalisation for the 100 companies on the index of over $400 Billion US. Given the size and number of other companies in this sector around the world, a conservative estimate would be to double this figure.

8.5. *Personal Information Economies*

8.5.1. Surveillance is not just conducted by states and organisations but also by ordinary people. After the bombings in London in 2005, both television companies and police were encouraging people to use their mobile phone cameras to take pictures of suspicious characters. Growing numbers of people, particularly children and young people, are also putting their lives up for display, and in turn watching others' lives, though online webcams[32] and social networking sites like *MySpace* and *Bebo*.

8.5.2. At the same time, those with greater access to knowledge resources are realising that it pays to try look after the 'data double' that is created by the multiple forms of surveillance that we undergo. This has become critical for life-chances, especially as credit scoring and other forms of database-driven rankings of the worthiness of individuals becomes the basis for the provision of a whole range of services. Credit referencing agencies offer online access to their credit-referencing records for individuals, allowing people to challenge and correct misleading data. This combination of voluntary corporate openness and the self-educated individual cannot be relied upon as a form of regulation, notwithstanding that a new generation of young people may be growing up as citizens used to carrying out, being subject to, and dealing with surveillance.

9. Surveillance Technologies

9.1. In our survey of surveillance technologies, we will first consider the vital importance of ordinary non-technological surveillance, before making some general but important points about the development and spread of surveillance technologies. We will then concentrate on linked and overlapping advances in four technological areas: telecommunications; audiovisual recording; digital computer technologies; and tagging and tracking technologies. We will also consider interconnections between different technologies and the trend for surveillance technology

[31] *SecurityStockWatch.com 100 Index,* August 2006, http://www.securitystockwatch.com/
[32] Koskela, H. (2004) 'Webcams, TV Shows and Mobile phones: Empowering Exhibitionism', *Surveillance & Society*, CCTV Special (eds. Norris, McCahill and Wood), 2(2/3): 199-215, http://www.surveillance-and-society.org/cctv.htm

simultaneously to vanish and spread everywhere. We will conclude by considering the limits of technological development and the consequences of technological dependence for organisations and government. There is, of course, much more: this section illustrates some major developments but cannot be exhaustive.

9.2. *Non-technological surveillance*

9.2.1. Whilst much attention focuses on advanced technologies of surveillance, it should not be forgotten how many basic and human forms of surveillance have been important throughout history, from the ancient act of 'eavesdropping' onwards, and are still important within contemporary society. These include: simple observation, watching, listening and following, both from law enforcement and private individuals; the use of human spies, undercover operatives and informers by police and security services; a whole range of medical, social security, financial and recruitment procedures based on face-to-face interviews; and the keeping of records on paper files. Some of the most intensive authoritarian surveillance regimes have been constructed around not much more than these basic ingredients usually combined with a strong sense of mistrust, and fear of infiltration, persecution or invasion. Examples can be found in pre-Second World War Germany and Japan, and the former Eastern Bloc countries, in particular the German Democratic Republic, which at one time employed up to one sixth of the population as informants. [33]

9.2.2. Two other routine and human forms of surveillance make amongst the biggest impact on citizens' lives: the breathalyser testing of those suspected of drink driving and the stopping and searching of people who might have been involved in crime. Whilst these may involve technologies, both rely fundamentally on human judgement (of police officers) in making the initial selection of whom to stop. However the reliance on human judgement also means that stop and search powers do not impact on all sections of the community equally, with black people in Britain being six times more likely to be stopped and searched than white people.[34]

9.2.3. Simple forms of surveillance may be more effective at providing positive protection and security than technologically-reliant methods. For example, in the UK, the lack of clarity about the primary purpose of the proposed national ID system is a key issue.[35] It is far from clear that even national security will be enhanced through this technology, and that it would perhaps be better served by improving border security and conventional intelligence gathering, underscored by the August 2006 alleged Atlantic flight terrorist plot involving more than 20 Britons.[36] Although the US Administration claimed that the operation showed the need for more advanced passenger data,[37] the alleged plot was foiled by the use of informers, undercover agents and tip-offs, and it is hard to see how advanced ID systems would have provided anything more effective.

9.3. *Technological Development*

[33] Garton Ash, T. (1997) *The File: A Personal History*, New York: Vintage Books.
[34] Home Office (2006) 'Operational Policing – Impact: about the Programme', viiii. http://police.homeoffice.gov.uk/operational-policing/impact/impact-about-the-programme/
[35] House of Commons Select Committee on Science and Technology (2006) *Identity Card Technologies: Scientific Advice, Risk and Evidence*, http://www.parliament.uk/parliamentary_committees/science_and_technology_committee/sag.cfm
[36] See: 'Special report: terrorism threat to Britain', *The Guardian*, 2006, http://www.guardian.co.uk/terrorism/0,,873826,00.html
[37] 'Government Seeks to Expand Data Collection on Airline Passengers' 22 August 2006, *New York Times*, http://www.nytimes.com/2006/08/22/washington/22data.html?ex=1313899200&en=1985587a17e2fbaa&ei=5090&partner=rssuserland&emc=rss

9.3.1. It is indisputable that new technologies have helped to change the nature of surveillance. Several general observations should be made about surveillance 'technology'. First of all, there is no inherent 'good' or 'evil' within these technological systems. Historically, IBM's punch-card machines were as essential to the efficient operation of the massive system of population surveillance that enabled the Nazis to single out Jews and other 'undesirables' for imprisonment and extermination, as early computers were to cracking the Enigma codes that sped the Allied defeat of the Nazis. Efficient national databases can be used for the provision of targeted health care or for the victimisation of political opponents.

9.3.2. However it is not a simple matter of how surveillance technologies are used. All technologies are developed within particular organisations which have particular aims. A technology can sometimes be appropriated by users, for example with text messaging on mobile telephones, which was never intended as their major purpose. However the capabilities of technologies are determined by the functionality built-in by their developers, for example the built-in surveillance of television viewing preferences of many TV-on-demand systems like TiVo). As we have seen, many technologies operate as part of global networks, and the parameters of the networks are controlled by corporations, state and often the military, for example, the Global Positioning System (GPS).

9.3.3. Several particular technologies and their capabilities will be examined below. However attention has to be paid not only to the capabilities and practical use of any technology, but also to the development process, the control over its operation as part of a network, and the way it connects to other technologies.

9.4. *Telecommunications*

9.4.1. Surveillance in telecommunications refers to the degree to which individuals, organisations and corporate bodies are able to monitor, sort and store information about the occurrence and content of telecommunications exchange, both between technological devices, and between technological devices and people. 'Telecommunications' includes the infrastructural technological processes of communication, the systems and devices through which telecommunications are achieved and also the exchange of 'data', 'messages' or 'information'. Included in current definitions of telecommunications are not only analogue but digital signal formats, and telecommunications includes not only fixed line telephony with voice calls and faxes, mobile telephony and the huge range of communicative functions enabled by large scale digital and computing systems such as the Internet.

9.4.2. Historically, the telecommunications infrastructure in the UK was dominated by fixed line cable telephony run by the state General Post Office. The single most likely source of surveillance was 'wiretapping', most often associated with state law enforcement. Three key developments have seen a radical transformation of this system: the expansion and convergence of telecommunications technologies, the development of information storage and processing capacity, and the diversification of telecommunications markets.

9.4.3. Throughout the last two decades, technological development and change has led to more diverse technologies employed for telecommunications. For example, radio frequency devices now enable large-scale cellular or mobile

telephony;[38] optical fibre cabling enables high-speed digital fixed internet connection, and a combination of both enable wireless computing. Mobile telephony delivers not only voice calls but text, image and video messaging, as well as location-based services.[39] Internet technologies enable both asynchronous communications such as email, bulletin boards and newsgroups, as well as synchronous communications such as chatrooms, instant messaging and webcam/video messaging.[40] Furthermore, current changes in the technologies of communication entail the convergence of technologies, and their interoperability. Internet connection can now be made via a range of devices, including handheld devices and mobile phones, and with the advent of VoIP (voice over internet protocol), voice calls can now be made via the desktop computer.

9.4.4. With the development of each of these different technologies have come the mechanisms for their use in surveillance. For any of these technologies to 'work,' they require the exchange of signals or data between technological devices, and any exchange of data itself generates the mechanisms for the capture, monitoring and storage of information about that exchange.

9.4.5. In mobile telephony, for example, the location of a mobile device can be ascertained simply by triangulating the signal of the device with its reception by a number of different base stations as the signals are 'handed over' from one to another – this information can be stored for later data-mining. As telecommunications technologies become more interconnective, extensive and intensive, the gathering, the potential for surveillance, and the storing and mining of information derived through them grow exponentially. The *routine* and automated collection of data on such a scale applies equally to the fixed line telephone and internet communications (internet telecommunications data being held on servers by Internet Service Providers). Furthermore, in February 2006, an EU directive on Data Retention and UK legislative initiatives from the Home Office have proposed to require not only mobile telecommunications companies, but those offering both fixed line telephony and Internet services, to retain data collected for up to two years in order that they be available for scrutiny by law enforcement bodies.

9.4.6. Transnational state surveillance of telecommunications, signals intelligence (SIGINT) remains an area shrouded in secrecy, with the technological capabilities the subject of a combination of educated guesswork, extrapolation and rumour. States also routinely filter vast amounts of telephone, telex, e-mail and fax traffic for reasons of 'national interests' (both security and economic interests). The so-called 'ECHELON' system, the global surveillance network operated by the American National Security Agency (NSA) maintains a huge base at Menwith Hill in North Yorkshire, which routinely automatically filters all telecommunications traffic passing thorough the UK for key words and phrases and increasingly employs more sophisticated algorithms for advanced speech and even meaning recognition[41]. International Licensed Cable (ILC) communications are perhaps one of the easiest forms of communications to intercept as for historical reasons all lines pass through nodal points located

[38] Radio also enables RFID (radio frequency identification) for tracking goods, services and, potentially, people.
[39] Location-based services in mobile telephony include global satellite information and positioning systems.
[40] Internet functionalities such as web pages and web logs are excluded here as they are ostensibly 'published', and therefore freely and publicly available as a matter of course.
[41] Campbell, D. (1999) *Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: Interception Capabilities 2000*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme; Wood, D (2001) The Hidden Geography of Transnational Surveillance, Unpublished PhD Thesis, University of Newcastle, UK.

in major cities. London is therefore a major centre for the interception of ILC communications, carried out by the UK's General Communications Headquarters (GCHQ) through a massive computer known as Dictionary.

9.5. *Video Surveillance*

9.5.1. Photographic surveillance has been inexistence longer than most people think. Almost as soon as it was invented, the camera was being used to record the faces and other physical characteristics of criminals.[42] Even television and video surveillance using Closed-circuit Television (CCTV) was used temporarily in public open streets in Britain as far back as the coronation of Elizabeth II in 1953 and permanently in some areas on London from the late 1960s[43].

9.5.2. Following the most recent surge of CCTV installation from the early 1990s, prompted by attempts to reverse the decline of city centre shopping districts as well as fear of terrorism, crime, there may now be as many as 4.2 million CCTV cameras in Britain: one for every fourteen people,[44] and a person can be captured on over three hundred cameras each day.[45]

9.5.3. During the 1990s the Home Office spent 78% of it crime prevention budget on installing CCTV[46] and an estimated £500M of public money has been invested in the CCTV infrastructure over the last decade.[47] However a Home Office study concluded that 'the CCTV schemes that have been assessed had little overall effect on crime levels'.[48]

9.5.4. Digitisation has allowed increasingly automated use of CCTV systems. So far this has occurred largely on the roads. Vehicle number plates are being used to identify the registered owner. Camera based enforcement of speed restrictions increased from just over 300,000 in 1996 to over 2 million in 2004 and raising an estimated £113 million in fines per annum.[49] This increase in state surveillance has received a consistently negative press,[50] despite the fact that speed cameras, unlike open street CCTV have a significant impact in reducing death and injuries cause by traffic accidents.[51]

9.5.5. The intensification of surveillance of the motorist is set to expand rapidly. In March 2005, the Association of Chief Police Officers demanded a national network of Automatic Number Plate Recognition (ANPR) 'utilising police, local authority, Highways Agency, other partner and commercial sector

[42] Sekula, A. (1986) The Body and the Archive, *October* 39: 3-64; Finn, J. (2004) Photographing fingerprints: data collection and state surveillance, *Surveillance & Society* 3(1): 21-44. http://www.surveillance-and-society.org/Articles3(1)/fingerprints.pdf
[43] Williams, C.A. (2003) 'Police surveillance and the emergence of CCTV in the 1960s', *Crime Prevention and Community Safety* 5(3): 27-38.
[44] McCahill, M. and Norris, C. (2003), 'Estimating the extent, sophistication and legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press.
[45] Norris, C and Armstrong, G. (1999), The Maximum Surveillance Society: The Rise of Closed Circuit Television, Oxford: Berg.:42
[46] *ibid*.: 54
[47] Norris, C. (2006) 'Closed Circuit Television: a review of its development and its implications for privacy', paper prepared for the Department of Homeland Security Data Privacy and Integrity Advisory Committee quarterly meeting, 7 June, San Francisco CA.
[48] Gill, M. and Spriggs, A. (2005). *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate, 43, 60-61.
[49] Wilkins, G. and Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D. Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office.
[50] McCahill and Norris, 2003 *op cit.* n.44.
[51] PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary

cameras'[52] including the integration of the existing town centres and high street cameras[53], with a National ANPR Data Centre, with an operational capacity to process 35 million ANPR reads every day increasing to 50 million by 2008, stored for two years.

9.6. *The Database*

9.6.1. It is this storage capability that has formed perhaps the biggest change already brought about by the information technology revolution: the ubiquity of the computer database. Multiple data can now be gathered, tabulated and cross-referenced far faster and more accurately than with the paper files that were once the characteristic feature of modern bureaucracy.

9.6.2. The collection, use and communication of large stores of personal data held on citizens are now central to the functioning of private business and the public services. Different data sets may be matched against each other to identify persons and suspicious patterns of activity. The data may also be 'mined' – analysed in great depth by sophisticated technologies to reveal patterns that may require further investigation.

9.6.3. The surveillance that is involved in the public service can be usefully thought of in terms of 'dataveillance', 'the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons'.[54] That term, a variation of 'surveillance', emphasises the importance of databases, rather than visual or auditory means of watching over people, in the practices of states and companies. Databases combined with other surveillance systems also allow algorithmic surveillance, the use of software to work on captured images or data and compare them to those in the database. This has been essential in the development of biometrics (see below).

9.6.4. In the private sector, the decreasing costs of databases and the increasing ability to extract actionable knowledge and value from data has resulted in a personal information economy in which many corporations seek to gather as much consumer data as possible.[55] Consumer data can be divided into four categories[56]: *Geographic* data describes features of place, demarcated by telephone area codes, postal codes, internet URLs and domain names. This is almost always connected to *demographic* data about individuals as 'geodemographic' data. *Psychographic* data concerns more social aspects of consumers in terms of class, values, lifestyle, life stages, and personality. Finally there is data on *consumer behaviour*.

9.6.5. Data are created and collected in many ways. Every transaction provides a 'data trail', linkable to an individual or type of person.[57] These transactions include the use of credit cards, bank cards, mobile phones, the Internet, a purchase, search or phone call. Additional data are generated through loyalty card programmes, customer surveys, focus groups, promotional contests,

[52] *ibid.*: 6
[53] *ibid.*:18
[54] Clarke, R. (1991 [1987]) 'Information technology and dataveillance', http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html
[55] See: Dyson, E., Gilder, G., Keyworth, G. and Toffler, A. (1996) 'Cyberspace and the American dream,' *The Information Society* 12: 295-308; 6, P. (2005) 'The personal information economy: trends and prospects for consumers,' in Lace, S. (ed.) (2005) *op cit.* n.6.
[56] These categories are drawn from: Michman, R.D. (1991) *Lifestyle Market Segmentation*. New York: Praeger; see also: Elmer, G. (2004) *Profiling Machines*. Cambridge, MA: MIT Press.
[57] Cash transactions for example, though usually unable to be linked to a consumer directly are often analysed against similar past transactions and types of consumers who have made these purchases.

product information requests, call centre contacts, web site cookies, consumer feedback forums and credit transactions. This *internal* and frequently proprietary data is often 'overlaid' with *external* data from state agencies (e.g.: National Statistics), non-profit organizations or specialist data collection companies. This rapidly growing business sector gathers data by combining publicly available data (for example, the census and the phone book), with data produced by promotional contests, warranty information (complete with extensive surveys), door to door, telephone, and shopping centre surveys, media and informational subscriptions and track web page traffic. These are most readily connected to postal codes, and given streets are 'profiled' with terms like 'prudent pensioners', 'fledgling nurseries' to 'rustbelt resilience.'[58] Profiles provide the means for companies to target their marketing to a narrower band of consumers, for example, a bank that has an agreement with a travel company may be able to market family holiday destinations to those it has categorized as families, with a different set of travel options to those who are retired.[59] Third party vendors may also provide lists of consumers who enjoy gardening (perhaps based on a magazine subscription) or of purported frequent travellers (perhaps drawn from survey research). The connections made between these sets of data are a result of 'data-mining' techniques designed to extract 'clusters' of data indicating patterns and relationships within a particular set of data.

9.6.6. Simple matching techniques and the use of geodemographic profiling is now augmented by more sophisticated 'heuristic' (learning) processes of data mining, often referred to as Knowledge Discovery in Databases (KDD). This further assists in discovering previously unknown and *non-obvious* relationships within sets of information.[60] The 'product' of these systems is perhaps most visible as the basis for web personalisation systems, such as is employed by Amazon.com, which use multiple sources of data to predict the likely preferences of current shoppers.[61] These techniques enable both descriptions of patterns of behaviour and predictions for behaviour within a reasonable range of accuracy. They assume that a given customer will replicate the patterns of others before him whether or not these patterns are obvious or not. These models of consumer behaviour serve to demonstrate the propensity of consumers to buy certain products, respond to certain marketing campaigns, be at risk for attrition, become a credit risk, and more.

9.6.7. Database development and use now forms a key part of change in public services. For example, there has been massive investment in the use of personal information in health care. The National Health Service (NHS)'s IT programme, *Connecting for Health*, is the largest in Europe, and commitments have been made far into the future.[62] For the past decade, there have been great

[58] The former category is derived from the ACORN classification system by a company known as CACI and the latter two categories are MOSAIC classifications by Experian. More information about these products are available at http://www.caci.co.uk/acorn/ and http://www.business-strategies.co.uk/Content.asp?ArticleID=629 See also: Burrows, R. and Gane, N. (forthcoming) 'Geodemographics, software and class.' *Sociology*.

[59] Again, there are privacy limitations to the use of this information and the sharing between companies, yet certain clauses do allow for this scenario to occur, particularly if the marketing material comes directly from the primary data owner, in this case, the bank.

[60] For more on distinctions between KDD and data-mining, see Tavani, H.T. (1999) 'KDD, data mining, and the challenge for normative privacy.' *Ethics and Information Technology* 1: 265-273. Many sources discuss data mining as the overall process of working with data for the purposes described here. See Rygielski, C., Wang, J-C, and Yen, D.C. (2002) 'Data mining techniques for Customer Relationship Management.' *Technology in Society* 24: 483-502, Danna and Gandy (2002) *op cit.* n.6. For the purposes of clarity, the term KDD is used here to define the overall technical process that indicates particular affinities (obvious or not) within sets of data and data mining as the practice of accumulating critical data for further data analysis.

[61] Fink, J., and Kosba, A. (2000) 'A review and analysis of commercial user modeling servers for personalization on the World Wide Web.' *User Modeling and User-Adapted Interaction* 10: 209-249.

[62] The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report*, London: H.M.Treasury.

efforts to co-ordinate, and to develop Electronic Patient Records (EPR), moving ultimately towards a comprehensive national digital database of all personal health records. The NHS 'spine' of data on each patient[63] is at the centre of the NHS Care Records Service, containing a limited amount of essential information that can be combined with a larger amount of locally-held care information. In addition, the programme involves national databases with patient records supplied by local NHS bodies, including data on notifiable diseases and information held for clinical audit. Pathology and other test records can be filed electronically. Plans and partial developments also include booking appointments, prescriptions, electronic transfer of patients' records between GP practices, and other functions. EPRs are held and transferred securely, for they are encrypted with a public-key system, and are subject to rules that allow personnel in each NHS function to look at only those data that are relevant to that function. There have been some local pilot schemes in which patients manage their own records through the use of smart cards.

9.6.8. Databases are also crucial in law enforcement. Some two million people a year are arrested by the police in England and Wales. The Criminal Justice Act 2003 empowered the police to take fingerprint impressions and DNA samples from all arrestees with the records remaining on police databases and accessible via the police national computer regardless of guilt or innocence. The database of fingerprints now contains nearly 6 million sets of prints and automated matching is almost instantaneous.[64] The National DNA Database was set up in 1995, has expanded so that 'virtually the entire active criminal population would be recorded on the database' by 2005.[65] In December 2005 the database held profiles on 3.45 million individuals, roughly 5.2% of the total population. Nearly 40% of black males are now profiled on the database compared with 9% of white and 13% of Asian males.[66] The Drugs Act of 2005, which became operational in March 2006, gave the police the power to drug test all people arrested for certain trigger offences, including theft, robbery, burglary and begging, again regardless of guilt.

9.6.9. The heart of the police IT infrastructure is the Police National Computer (PNC). The PNC holds a range of databases and provides the ability to read external databases such as the register of drivers held by the DVLC and is now linked to more than 30,000 terminals across the country. The last decade has seen the PNC moving from being an electronic filing cabinet to a fully-fledged intelligence tool in its own right with the ability to search across any of the fields.[67] It is now augmented by ANPR, the National Automated Fingerprint Identification System (NAFIS) and the Violent Offender and Sex Offender Register (ViSOR), which provides police and probation with a shared national database that contains an expanded set of information on offenders, including personal details, descriptive details, behavioural traits, details of risk assessment, intelligence reports, an activity log and a photographic library[68]. The most recent initiatives has been a project to develop a Facial Images National Database (FIND), to be fully operational by 2009, cross-referenced to

[63] NHS Connecting for Health (2006) 'Spine', http://www.connectingforhealth.nhs.uk/delivery/programmes/spine .
[64] PITO (Police Information Technology Organisation) (2005) *Annual Report 2004 – 2005*, HC 261, London Stationery Office.
[65] FSPU (Forensic Science and Pathology Unit) (2005) *DNA Expansion Programme 2000-2005: Reporting Achievement.* London Home Office:3, Postnote 200.
[66] Randerson, J., 'DNA of 37% of black men held by police', *The Guardian*, 5 January 2006, http://www.guardian.co.uk/frontpage/story/0,,1678168,00.html .
[67] *ibid*.
[68] PITO (2004) 'Memorandum by the Police Information Technology Organisation to the Bichard Inquiry', http://www.bichardinquiry.org.uk.edgesuite.net/10663/full_evidence/0018/00180001.pdf .

the PNC.[69] These databases are also used for Criminal Records Checks, which are now mandatory for persons seeking employment in jobs involved with the care of the young or vulnerable. Since 2002 it has produced 8.2 million disclosures of which around 400,000 contained convictions or police intelligence information.[70] These will be cemented by the Criminal Justice Exchange (CJX) system, which will enable information to be shared across all the agencies of the criminal justice system[71], not only at police stations but, with the development of Airwave, the new police digital communications system, the patrol officer on the street via a hand held computer.[72] Ultimately, the Cross Regional Information Sharing Project (CRISP), will create a single national police database will integrate all databases on the PNC with those held locally.[73]

9.6.10. With the development of the National ANPR Strategy the database is set to become an even more central feature of routine policing. For instance, under the ANPR strategy there is a plan to link garage forecourt cameras to the system, which will greatly increase the coverage of the system since, at some point, all vehicles must fill up with petrol. In exchange, the petrol stations will 'benefit from our intelligence telling them which vehicles to take payment from before they serve them'[74]

9.6.11. In border surveillance practices concerns there has been significant data-led restructuring of the role of the border guard. The proliferation of 'smart borders' and 'electronic borders' have at the heart of their vision, the repositioning of border guards as 'the last line of defence and not the first'.[75] The everyday experience of surveillance at the border, then, is preceded by a dataveillant system that makes judgements about degrees of risk before the physical border checkpoint.

9.6.12. This is not only the case in the mobility of people, but also in the mobilities of money and goods.[76] The UN's Financial Action Task Force (FATF) for intercepting terrorist finances, for example, envisages stopping the money before it reaches the border. As analyses have shown, however, the war on terrorist finance has resulted in greater surveillance of cross-border money transfer agencies such as Western Union and, by implication, the money transferred by migrants as remittances to their country of origin. An important issue here, then, is how data are used to pre-judge the risk of a particular border crossing and whose lives are most significantly affected by such judgements.

9.7. *Biometrics*

9.7.1. All new ID systems also use some kind of biometric: fingerprints, iris-scans, facial topography and hand-scans are all used on different passports and ID card systems. The allure of biometrics is the appearance of an 'anchor' for identity in the human body, to which data and information can be fixed. The biometric identifier – iris scan, digital fingerprint, facial scan, voice biometric

[69] PITO (2006) *Facial Images National Database (FIND)*, http://www.pito.org.uk/products/FIND.php
[70] 'Criminal records mix-up uncovered', *BBC News*, 21 May 2006, http://news.bbc.co.uk/1/hi/uk/5001624.stm
[71] CJIT (Criminal Justice Information Technology) (2005) *CJS Exchange*, http://www.cjit.gov.uk/glossary/#c
[72] ACPO (Association of Chief Police Officers) (2002) *Infinet: A National Strategy for Mobile Information*, London: ACPO.
[73] Home Office (2006) *op cit.* n.34.
[74] ACPO (Association of Chief Police Officers) (2005) *ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road*, London: ACPO. http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc
[75] Accenture Digital Forum (2004) 'US Homeland Security to Develop and Implement program at air, land and sea ports of entry' http://www.digitalforum.accenture.com
[76] deGoede, M. (2003) 'Hawala discourses and the war on terrorist finance', *Environment and Planning D: Society and Space* 21(5): 513-532. Chalfin, B. (2004) 'Border scans: sovereignty, surveillance and the customs service in Ghana', *Identities: Global Studies in Culture and Power* 11: 397-416.

or hand scan – becomes the access gateway to the data held. It is this convergence of data-mining and information integration with biometric identifiers. The idea is that accuracy will be increased and fraud reduced. PINs and passwords may be forgotten or lost, but the body provides a constant, direct link between record and person.

9.7.2. Whilst biometrics had been growing rapidly, the 'War on Terror' has produced a massive surge in both research funding and implementation. After 9/11 in the USA, biometric techniques already in commercial use or on the threshold of applicability were fast tracked and heralded as the key to winning this new kind of war.[77] The US Patriot Act, in a framework that has implications far beyond US soil, established a set of practices for biometric applications that afforded their almost unlimited use in the investigation and identification of terrorist activity.

9.7.3. In British cities, following early experiments of face recognition software in Newham, Birmingham, Tameside, Manchester, and other locations, as well as in the United States, however, a shift towards digital CCTV, which uses computer algorithms to search automatically for stipulated people or behaviours, is gaining momentum. Face recognition, and other biometric CCTV systems, still face major technical obstacles in operating outdoors on city streets. However, considerable research and development investment is rapidly addressing these.[78]

9.8. *Locating, Tracking and Tagging*

9.8.1. Surveillance practices are increasingly referenced, organised and located through Geographical Information Systems (GISs)[79]. Many actually track the geographical movements of people, vehicles or commodities using RFID chips, Global Positioning Systems (GPS), smart ID cards, transponders or the radio signals given off by mobile phones or portable computers.

9.8.2. According to a forensic engineer cited in a BBC report, mobile traffic data can link suspects to crimes: 'if a person makes a mobile call, potentially while involved in commission of a criminal act, it is possible to determine from [the traffic data] where the radio footprint would have been made.'[80] There is frequently no differentiation between the mobile as a device and the mobile user. According to the Home Office, 'communications data is an important investigative tool: allowing investigators for example to establish links between suspected conspirators (itemised bill) or to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi (cell site analysis)'.[81]

9.8.3. Both GPS and RFID are increasingly being seen as solutions in law enforcement and personnel management. Electronic monitoring has also been introduced as a condition of being granted bail and in 2004/5 some 631 adults and 5751 juveniles, some as young as twelve years old, were 'tagged' allowing

[77] Amoore, L. (2006) 'Biometric borders: governing mobilities in the war on terror', *Political Geography* 25: 2: 336-351; Gates, K. (2005) 'Biometrics and post-9/11 technostalgia', *Social Text* 23(2): 35-53. Irma Van der Ploeg, 'Biometrics and the body as information', in Lyon, D. (ed.) (2003) *op cit.* n.6.
[78] See Norris, C. (2003) 'From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control,' in Lyon, D. (ed.) (2003) *op cit.* n.6; Norris, C. and Armstrong, G. 1999: *The Maximum Surveillance Society : The Rise of CCTV*, Oxford: Berg.
[79] Institute for the Future (2004) *Infrastructure for the New Geography*, Menlo Park, CA: IFTF.
[80] 'Phone firms 'flooded' by crime checks'. *BBC News*, 20 December 2002, http://news.bbc.co.uk/1/low/uk/2592707.stm
[81] See Home Office (2006) *Surveillance: Access to Data*, http://security.homeoffice.gov.uk/surveillance/access-to-data/

them to await trial at home rather than be remanded into custody.[82] Offenders released from prison are also increasingly subjected to electronic monitoring either as a condition of early release from prison under the Home Detention Curfew Scheme[83] or as a condition of being released on Parole.[84]

9.8.4. RFID underpins new 'smart' means of continually tracking goods and people wirelessly as they move across geographic environments. These chips emit a limited range radio signal that can be picked up by receivers usually within a few centimetres. One other major distinction here is active versus passive RFID. Increasingly the possibilities of the use of active RFID are on the agenda. Indeed, recent high profile bids for government border security contracts have included demonstrations of the potential of wireless tracking devices.

9.8.5. Until recently their use has been restricted to large shipping containers, consumer goods and various kinds of 'smart cards'. In the US, despite serious challenges to proposals for RFID in passports and visas, RFID-enabled border smart cards are being trialled at the US-Mexico border. On the supply side, the RFID industry is flagging the potential for the technology to allow the tracking or tracing of migrant workers who cross the border for a time-limited period.

9.8.6. Recently a notable change has occurred subtly and largely unnoticed: the implantation of living beings. While race-horses were the first, mass microchipping of animals has began with chips containing information about immunisation records and ownership gradually replaced quarantine requirements for household pets in the EU from 28th February 2000 through the PETS scheme, which has since been extended beyond Europe[85].

9.8.7. The first human use of RFID chips has been in elderly people suffering from degenerative diseases in the United States, and around 70 people with degenerative brain conditions have now been implanted to enable carers to locate them easily[86]. Researchers and technological enthusiasts have also been implanting themselves with chips for several years[87], and at least one chain of Spanish nightclubs has offered patrons the chance to have cash and access privileges held on implanted chips[88]. However a step-change occurred in February 2006 when a security company on Ohio, USA, implanted two of its workers with RFID chips to allow them to access company property[89]. Although such an invasive procedure was carried out voluntarily, it raises enormous questions of the integrity of the body and privacy in relation to employers. It is also not entirely surprising that the call for everyone to be implanted is now being seriously debated on some technology websites.

---

[82] NPS (National Probation Service) (2006) *Electronic Monitoring* 6. http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes .

[83] The HDC scheme allows for those sentenced to between 3 months but under four years imprisonment to be released between 2 weeks and four and a half months early on a curfew enforced by electronic monitoring. In 2004/5 19096 people were release early under the scheme (*ibid.*: 6).

[84] NPS *op cit.*

[85] For details, see: DEFRA (Department of Environment, Food and Rural Affairs) (2006) *Pet Travel Scheme,* http://www.defra.gov.uk/animalh/quarantine/pets/index.htm .

[86] The company involved is Verichip Corporation. http://www.verichipcorp.com/ .

[87] Amal Graafstra is one such high profile enthusiast and advocate of self-chipping. Explanations, pictures and videos can be downloaded from his website http://amal.net/rfid.html .

[88] Graham-Rowe, D. (2004) 'Clubbers chose chip implants to jump queues', *New Scientist*, 21 May, http://www.newscientist.com/article.ns?id=dn5022 .

[89] Waters, R. (2006) 'US group implants electronic tags in workers', *Financial Times*, 12 February. http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html .

9.8.8. Commercially, both RFID tags and GPS are seen by companies as a means to produce customised marketing in real time to particular consumers, offering discounts on mobile devices to retail outlets in a given location, for instance. However both RFID and GPS use have been hindered by the costs of the technology compared to the costs of the products to which they are attached. Applications for these have largely been a part of personnel and inventory management, both forms of workplace surveillance, yet as these technologies continue to become less expensive it remains likely that these location tracking devices, especially RFID chips, will be used to monitor both consumer products and consumers themselves.[90] Continued developments in the application of real time geographic data to consumer profiles will provide yet another layer of data to assist corporations in targeting marketing campaigns to particular consumers. These, therefore, are technologies whose functions are highly likely to 'creep.'

9.9. *Technological Synergy and Function Creep*

9.9.1. Whilst the capabilities of individual technologies and systems are important, there is also increasing technological synergy, or convergence of surveillance technologies. This is a long-term trend within computer systems and is also motivated by desires to create economies of scale. More and more systems are designed with interoperability in mind. This also means that new products can emerge out of older technologies, which in themselves had been understood and managed by regulators, coming together to create an entirely unforeseen and unregulated function.

9.9.2. This interoperability and technological synergy can be added to the more simple but common 'function creep' as multiple new uses are found for technologies and as information gathered for one purpose or in one domain leaks through into others. For example, not only are the same data-mining techniques developed for profiling consumers being used by security and intelligence services to profile potential terrorists, often the very data from which these profiles are created are the same. There is also some evidence now that the dominance of a particular firm in commercial applications of a technology (for example fingerprint secure entry systems for workplace security) is a key factor in their success in security procurement processes. In the workplace, employee monitoring technologies can sometimes yield more information than intended, and management has the temptation to extend monitoring practice without consulting employees. This can be particularly important if the information is being used in decisions about pay or promotion.

9.9.3. Pressure is on to find IDs that work for several purposes – border crossing, fraud control, access to government information and perhaps commercial (video rental) and semi-commercial ones (libraries) as well – which is shaping the field in fresh ways. The key problem is that once established, systems can easily acquire an apparent life of their own which is much easier to initiate than to halt or redirect. When agendas such as the 'war on terror,' curbing the migration of undesirable groups and even the quest for solutions for credit card fraud are shaping the development of ID systems, the 'impersonal' ethos of a classic bureaucracy do seem somewhat undermined. The chief difficulty lies in the powers granted to the state (and corporate and technical bodies) controlling the means of identification.

[90] See: Lyon, D., Marmura, S. and Peroff, P. (2005) *Location Technologies: Mobility, Surveillance and Privacy, Queens University*, Kingston, Ontario: The Surveillance Project. http://www.queensu.ca/sociology/Surveillance/files/loctech.pdf .

9.9.4. Other examples include the London congestion toll system, which has been enrolled as part of an anti-terrorist initiative proactively searching for suspect and stolen cars. The story of ANPR in London also shows that function creep works in several ways: the technology was originally developed for military purposes, installed to help identify IRA bombers, and now has a role in traffic management, local government revenue raising and security against a new generation of terrorists.

9.9.5. In medical surveillance, diagnostic surveillance technologies can move from individual diagnostics towards ever broader surveillance, applied to larger and larger proportions of the population. In particular they have a tendency to creep into forensic purposes. A number of technologies used for medical diagnosis have also been applied to forensics – DNA analysis of tissue fragments; analyses of bodily performances such as posture, gait, or facial expression; analyses of body parts and images or imprints (e.g. fingerprints, height, weight, bodily proportions). Many of these are now being proposed for surveillance purposes in the form of extensive databases against which identities can be checked.

9.9.6. With traffic or transmission data, organisations are entirely free to gather, store and manipulate what data they will (and are now required by law to retain it for longer periods of time). This clearly leaves the sector open to function creep in the surveillance of telecommunications data, and where the state and corporate sectors are each extensively involved, data subjects have little power with respect to the ways their data are collected, stored, shared, bought or sold.

9.10. *Towards Pervasive Surveillance*

9.10.1. Technologies are at their most important when they become ubiquitous, taken for granted, and largely invisible. As Mark Weiner argued in 1991, 'the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it'.[91] Digitised, networked surveillance technology is tending towards pervasiveness. Pervasive or ubiquitous computing (Ubicomp), also known in Europe as 'ambient intelligence' (AmI), creates the conditions for pervasive or ubiquitous surveillance.[92] One of the fundamental building blocks of Ubicomp is the concept of the Uniform Resource Locator (URL), known to most people through the use of Internet addresses. However a URL was always intended to be much more than this, it is supposed to provide a place in the network for potentially all objects and people.

9.10.2. Such continuous software-sorting of people and their life chances in cities is organised through myriad electronic and physical 'passage points' or 'choke points', negotiated through a widening number of code words, pass words, PIN numbers, user names, access controls, electronic cards or biometric scans. Some are highly visible and negotiated willingly (a PIN credit card purchase or an airport passport control). Others are more covert (the sorting of internet or call centre traffic). On still other occasions, the passage point is clear (a CCTV camera on a street or a speed camera on a motorway), but it is impossible to know in practice if one's face or car number plate has actually been scanned.

[91] Weiner, M. (1991) 'The computer for the 21st century', *Scientific American*, 265 (September): 94-104.
[92] Kang, J. and Cuff, D. (2005), *Pervasive Computing: Embedded in the Public Sphere*, available from dcuff@ucla.edu. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57: 43-49.

9.10.3. Electronic services and realms are relatively easy to control compared to physical urban streets, but increasingly most passage points now involve *both* electronic and physical parts working closely together. The combination of CCTV, biometrics, databases and tracking technologies can be seen as part of a much broader exploration, often funded with support from the US/UK 'war on terror', of the use of interconnected 'smart' systems to track movements and behaviours of millions of people in both time and space. In industry parlance, this is called multiscale spatiotemporal tracking.[93]

9.11. *The Limits of Technology*

9.11.1. Of course, the promise of technologies is almost never delivered quite as anticipated. The biometric technologies for the USVISIT programme, for example, were downgraded from planned iris scans to digital fingerprints for logistical reasons. Similarly, the biometrics elements of the UK's e-Borders programme have been subject to problems of implementation. As a result, the biometrics elements of routine border surveillance practices are relatively underdeveloped.

9.11.2. Some of these problems concern reliability[94] with outstanding problems of 'failure to enrol (FTE)' (the biometric is unrecognisable) and 'false non-match' (subsequent reading does not match the properly enrolled individual biometric). Despite this, major implementation decisions are often made before full trials have occurred. For example in the proposed UK ID system, it has been estimated that as many as one in six persons may not be able to use their ID cards because of the FTE problems.[95]

9.11.3. Whether a medical diagnostic, forensic or any other surveillance technique involving the probabilistic and/or predictive identification of targets yields false non-matches depends on two important elements: the *sensitivity* and *specificity* of the technology used. **Sensitivity** is the technology's ability to identify relevant cases correctly. **Specificity** (also called **selectivity**) is the technology's ability to exclude irrelevant cases correctly. Individual characteristics, organizational settings, test criteria, and domain-specific knowledge will yield different sensitivity and specificity outcomes. Sensitivity and specificity values also depend on the criteria set for the test for example whether ultrasound scans for Down's syndrome in foetuses is carried out by a skilled or semi-skilled operator) and they tend to trade off against each other. Widening sensitivity means identifying a higher number of potential targets, but within that (necessarily) larger identified population there will be a higher number of borderline and falsely identified targets, so selectivity decreases. Hence no test is perfect, and the setting of sensitivity/specificity thresholds is as much a product of political, social and organizational factors as it is the technology. As such, it is wise to assume that a certain percentage of an identified population will be false negatives or positives. There are hence more values to discuss: the *positive and negative predictive values* of the test. Positive predictive value is the percentage of true positives among all test positives, negative predictive value correspondingly the percentage of true negatives among all test negatives. The predictive values of a test depend on the accuracy of the indicators on which the test is based.

[93] Hampapur, A. *et al.* (2005), 'Smart video surveillance', *IEEE Signal Processing Magazine*, March: 38-51.
[94] See: Zureik, E. with Hindle, K. (2004) 'Governance, security and technology: the case of biometrics' *Studies in Political Economy*, 73: 113-137.
[95] See: Grayling, A.C. (2005) *In Freedom's Name: The Case Against Identity Cards*, London: Liberty.

9.11.4. As the accumulation of personal data enables predictive, pre-emptive and preventative surveillance to occur in a wider variety of settings, the imperfections in statistical methods could have far-reaching consequences for those falsely identified. Such errors can do even more than limit access to places or services: in medical surveillance, they may be life-threatening, and they are far more common than most people realise. And in fact only the newest forms of biometric technologies – e.g. DNA typing and facial recognition – have been submitted to testing that give us some basis for estimating error rates, and the methodologies used for estimating error rates are less precise than those used for medical technologies. The best system tested by the US military's Facial Recognition Vendor Tests (FRVT) in 2002 reached only 74% identification under ideal conditions, and this test did not deal with more complex issues of the prevalence of faces being looked for within a population. Facial recognition cannot under realistic circumstances provide any kind of reliable security even against known terrorists.

9.11.5. For DNA, it has been assumed even in courts that DNA identification is in fallible. However for forensic identification purposes, only a few small segments of the entire DNA string are tested and only series of repeated base pairs (called 'stutters') within the so-called 'junk' DNA are shown in the so-called profile. However whilst a negative DNA test seems to be near perfect tool for acquitting the innocent, false negatives being very rare, false positives are surprisingly likely and a positive DNA test might be met with far more scepticism than occurs in courts.

9.11.6. Even less complicated recognition technologies like ANPR systems are not 100% accurate in reading number plate details[96] which means, inevitably, that information in the database will be compromised, and that the system may well lead to a person's vehicle being wrongly identified as associated with known criminals. This issue of misidentification on police databases was most recently illustrated when the Criminal Records Bureau revealed that around 2,700 people have been wrongly identified as having criminal convictions. As a consequence of the incorrect information contained in their data-doubles, a number were refused jobs. The problem of the quality of the data held on the PNC has been highlighted by a number of reports from the Police Inspectorate;[97] the most recent noted that 22% of records input to the PNC at force level still contained an error, even when checked by a supervisor.[98] The prospect of the National Police database also brings dangers as low-grade intelligence of uncertain provenance is made available more widely and used as the basis for risk based decision-making by various agencies.

9.12. *Technological Lock-in and Regulatory Lag*

9.12.1. Technological failure or inadequacy can therefore result in worse outcomes for life-chances than a successful technological system. However this cannot be used as an argument for the answer to be merely, 'better technologies'. Surveillance is the first port of call in response to any kind of problem is a strongly managerialist solution, frequently proposed to

[96] PA Consulting (2004) *op cit.* n.51, suggest that the accuracy read is around 96%, which may sound high, however, even if only one percent of licence plates are incorrectly read and recorded on the data base, this would mean potentially up to half a million erroneous number plates logged each day.
[97] See for example HMI Constabulary (2002) *Police National Computer: Data Quality and Timeliness, Second Report*, London: HMI Constabulary.
[98] HMI Constabulary (2006) *Police National Computer Compliance Report: Avon and Somerset Constabulary*, p.16, para 2.5.1 http://inspectorates.homeoffice.gov.uk/hmic/inspect_reports1/pnc-audits.html/a-and-s-pnc06.pdf?view=Binary

governments by management consultants who operate on measurement-based world views. Surveillance technologies therefore get promoted unproblematically as 'the answer' to multiple threats, most recently to the threat of terrorism. For example, one conservative American journal called for a dense urban infrastructure of automated software systems and micro-sensors: 'Dispersed along roadsides, hills, and trails, they will report just about anything that may interest us—the passage of vehicles, the odor of explosives, the conversations of pedestrians, the look, sound, weight, temperature, even the smell, of almost anything'[99].

9.12.2. However the more that states, organisations, communities and people become dependent on surveillance technologies, the more there is an apparent 'lock-in' which prevents other options from being considered, and a comprehension gap which increases a dependence on expertise outside the democratic system. ID cards are a key case in point and will inevitably increase our reliance on those providing both technological and commercial expertise. Whilst most politics now has technological components, regulators are constantly running behind technological innovation, unable to understand 'how it works'. There is therefore a significant regulatory lag resulting from the lack of knowledge and understanding behind technological development. In this constant chase, one has to ask whether states possess the necessary tools to carry out meaningful regulation of increasingly complex surveillance technologies and practices. The question that frequently arises with all technological development is whether 'the genie can be put back into the bottle'. Patent holders and vendors tend to be silent on the reversibility of devices and systems.

10. Surveillance Processes

10.1. Several key processes make up the operation of the surveillance society. As we have seen, one of the most significant developments is how surveillance, that was once reserved for the 'suspect' or 'deviant', has become extended to cover the majority of the population, which can then be sorted, categorised and targeted.

10.2. *Social Sorting, Categorisation and Targeting*

10.2.1. Social sorting can be observed in many areas: in the marketplace, consumers continually supply business with their consumption data, they are part of an evolving feedback loop that binds acts of consumption with the gathering of transaction-generated data.[100] Consumers have come to expect that forms of personal data will be required of them in economic transactions. Moreover, they are often rewarded for providing personal information, (for example, when they benefit from loyalty programs), but otherwise do not believe that consumer surveillance has any effect on their day to day lives. Yet in this process, consumers are implicated into a system that perpetuates and reinforces systems of stratification, building up categories based upon their participation.

10.2.2. In the workplace, the call centre industry is a key example. Call centres now rank order customer accounts according to their relative spend. The higher the spend, the greater a customer's value is to the organisation, and so when

[99] Huber, P.W. and M.P. Mills (2002) 'How technology will defeat terrorism', *City Journal* 12(1) http://www.city-journal.org/html/12_1_how_tech.html

[100] Detailed in: Elmer, G. (2004) *op cit.* n.56.

these customers call for service, they are routed into shorter queues and answered by more skilled employees. Moreover, the customer profile is seen as critical when recruiting call centre employees, who are now assessed for social and lifestyle competencies which match those of the market segment they are serving.

10.2.3. Telecommunications companies (Network Operators, Internet Service Providers, Content Providers) routinely gather and manipulate the personal data they hold about their own customers in a similar vein as do other private sector organisations, to sort and categorise those customers as consumers. Additionally however, for the private sector the distinction between restricted billing (personal) data and fully archivable traffic data is important, particularly for marketing campaigns, such as those conducted via SMS (short message service, or text).[101]

10.2.4. The mobile phone is regarded by consumers and the telecommunications industry as a personal communication device and this ability to enable interaction with users is what makes mobile data economically valuable. At the same time, the mobile phone number as index is treated as an impersonal piece of information. The index is nevertheless sufficiently precise to allow data mining techniques to find personal data out of supposedly impersonal data. Telecommunications surveillance by corporate entities therefore potentially sorts consumers by their economic value to the organisation, and may do so on the basis of unregulated transmission data, as well as the billing data protected under data protection legislation.

10.2.5. The climate of heightened national security concerns is also intensifying the drive to 'social sorting' at national borders.[102] Where people can verify their identity and authenticate their activities, arguably their experience of crossing borders is one of expedited travel, Of course, the trade-off here is the submission of personal data, biometrics and access to private information. At many air, sea and land ports of entry it is now common, for example, to see 'fast track' lanes for expedited crossing, for example the 'Privium' system at Schiphol Airport in the Netherlands, which uses an iris-scan in place of lengthy queues for passport control. Such privatised spaces of 'trusted traveller' experience, though, do raise questions of data protection and privacy. Moreover, the growth of expedited border security sorts people and transactions into categories of risk that allows greater surveillance to be applied to those who do no or cannot enter the private spaces.

10.2.6. Finally, the UK's proposed ID system would have the capacity to sort between those eligible for services or access, and others. Less-than-visible mechanisms will also operate, that skew the system against those already likely to be disadvantaged. It is this ability to engage in social sorting that may in the long term be even more insidious than the fears about reduced mobility in countries where police may demand ID documents at any time.[103] Such social sorting tends to produce second class citizenship rather than supporting a more solidaristic and egalitarian practice.

10.2.7. Categorisation involves sorting populations into categories and then rank ordering within and between those categories. It is at the heart of most scientific

[101] Green, N and Smith, S. (2003) '"A spy in your pocket?" the regulation of mobile data in the UK' *Surveillance & Society* 1(4): 573-587. http://www.suveillance-and-society.org/articlesv1i4/pocketspy.pdf .
[102] Lyon, D. (2003) *op cit.* n.7; Lyon, D (ed.) (2003), *op cit.* n6.
[103] Lyon, D. (2004) *ID Cards: Social Sorting by Database*, OII Issue Brief 2004; Oxford: Oxford Internet Institute.

and management practice[104]. And states and institutions have been using such systems for many years, from examinations and gradings to having prisoners, soldiers and others wear particular recognisable clothes (uniforms), and, in extreme cases such as Nazi Germany, in wearing signs of categories like the yellow star for Jews worn on clothes, and the tattooing of concentration camp inmate numbers on the skin.

10.2.8. One of the primary categories for the state is that of citizenship. Citizenship and surveillance belong together in the modern world. Extensive records on each individual are needed to inform government departments about who has a right to what.

10.2.9. Since the later part of the twentieth century, most of these records have been computerised and are increasingly linked and automated. The early twenty-first century has seen the development of several new national identification systems. The UK in Parliament in March 2006 approved plans, in response to 9/11 and the 'war on terror.' Citizen identification is not merely about cards. New national ID card systems, are based on a national registry, a database (or databases in the UK case) containing personal information that can be searched and checked independently of any demand to see the card held by the citizen. The unique identifier contained in the card is also the key to unlock the database(s) and thus is itself a source of considerable power.[105] . It makes it possible to obtain access to several kinds of database; the more multi-purpose the system the more databases are likely to be involved. If the UK ID card system is to guard against 'identity theft,' then commercial data relating will be accessible as well as government data.

10.2.10. Second, the public spaces and physical and electronic infrastructures of cities are rapidly being restructured in ways that directly exploit the capabilities of new surveillance technologies. On the way out are universal and standardised provisions of access to services, spaces and infrastructures, based on notions of democratic citizenship, open access or traditional ideas of public services and spaces either freely accessible to all at the point of consumption or charged through universal tariffs. On the way in are notions of targeted services, infrastructures and spaces, accessible only to these who are allowed access, and priced very differently to different people and places.

10.2.11. Profiles provide the means for companies to target their marketing to a narrower band of consumers, thereby decreasing marketing costs and increasing response rates. This is frequently far cheaper than mass marketing channels of television, radio or print marketing. For example, a bank that has an agreement with a travel company may be able to market family holiday destinations to those it has categorised as families, with a different set of travel options to those who are retired.[106] Third party vendors may also provide lists of consumers who enjoy gardening (perhaps based on a magazine subscription) or of purported frequent travellers (perhaps drawn from survey research). Continued developments in the application of real time geographic data to consumer

[104] Bowker, G. and Star, S. L. (1999) *Sorting it Out: Classification and its Consequences*, Cambridge MA: MIT Press.

[105] See e.g.: Clarke, R. (2006) 'National Identity Schemes: The Elements' http://www.anu.edu.au/people/Roger.Clarke/DV/NatIDSchemeElms.html

[106] Again, there are privacy limitations to the use of this information and the sharing between companies, yet certain clauses do allow for this scenario to occur, particularly if the marketing material comes directly from the primary data owner, in this case, the bank.

profiles will provide yet another layer of data to assist corporations in targeting marketing campaigns to particular consumers.

10.2.12. Geo-referencing of surveillance brings with it major risks. Services and advertising can be targeted only at those deemed more profitable. Commercial judgements, based on continuous connections to credit registers and the like, could lead to the regular exclusion and targeting of people deemed to be commercially marginal within increasingly commercialised and gentrified town and city centres.

10.2.13. For the police, the classification of a 'persistent' or 'prolific' offender is a statistical category determined by the number of convictions, over a particular period of time, an individual has accrued on the Nominal Index contained on the Police National Computer. This classification makes an individual a candidate for intensive targeting and intervention by a range of criminal justice agencies as part of the persistent offender strategy.[107] Once selected a candidate will be entered on the J-track system for tracking and managing persistent offenders at all stages of the criminal justice system.

10.3. *Unintentional Control*

10.3.1. However, whilst social sorting is both an intention and an outcome of many forms of surveillance, surveillance should not be taken to be identical with direct social control.[108] While social control, the strict regulation of personal behaviour to order society, can be the intention of surveillance (and has been historically), in most contemporary western cases the controlling effects of surveillance are indirect or unintentional.

10.3.2. The intention of surveillance is often simply to manage efficient and swift flows of goods, people and information.[109] This can mean people, for example in London, the Underground's Intelligent Pedestrian Surveillance (IPS) system[110] aims at identifying places where crowd flow is blocked, and the 'Oyster' smart card, used by 5 million Londoners to access London's public transport system, is aimed at speeding the movement of people through the city. It can mean people indirectly, for example, the congestion charge, which aim to reduce the numbers of cars on London streets through an ANPR system scanning car number plates for non-payers. Another example is the use of 'Customer Relationship Management' (CRM)[111] in marketing which actively seeks personal information about current and potential clientele in order to establish a continuing relationship that goes beyond a commercial transaction.[112] It can be entirely about goods: for example the use of Radio-RFID chips in shipping containers and consumer goods.

10.3.3. However, what spells 'efficiency' for one person spells 'social control' for another: this is particularly true for strongly personalised systems like ID

[107] Home Office (2004) *Prolific and Other Priority Offender Strategy Initial Guidance*, http://www.crimereduction.gov.uk/ppo_e.doc
[108] Lianos, M. (2001) *Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social.* Paris : L'Harmattan-Logiques Sociales.
[109] Graham, S. and Wood, D. (2003) 'Digitising surveillance: categorisation, space and inequality,' *Critical Social Policy*, 23: 227-248.
[110] Hogan, J. (2003) 'Smart software linked to CCTV can spot dubious behaviour', *New Scientist*, 11 July, http://www.newscientist.com/article.ns?id=dn3918 .
[111] CRM involves the electronic dispersion of personal data to analyze and create customised long term relationships with customers.
[112] Morgan, R.M., and Hunt, S.D (1994) 'The commitment-trust theory of relationship marketing,' *Journal of Marketing* 58: 20-38.

records retrieval, which involves consistent and unique identifiers for individual citizens.[113]

10.4. *Information Sharing*

10.4.1. To allow for social sorting, information needs to be accurate and readily available. In many countries, including Britain, there is a trend towards more integrated, 'joined-up' public services, often through partnerships and teamwork across several agencies. Increasingly, a variety of local partnership arrangements bring together a variety of agencies and professions so that their skills can be better focused on providing services to individuals in a more integrated way.[114] The heart of New Labour's modernisation agenda has been to transform a set of disparate agencies into a coordinated and joined-up system with a huge investment in IT provision.

10.4.2. One effect of this key development is that the boundaries that were once thought to have provided certain, albeit fragile, safeguards to privacy and limits to surveillance are called into question, often leaving both the public and the service-providers bewildered about how personal information is, and should be, managed. Personal data flow into new channels – some of them private – through organisations that never before had access to them, and whose traditions of confidentiality and privacy protection may differ substantially from each other, and from those of agencies in the public sector.

10.4.3. Combating fraud is a major example. The Social Security Administration (Fraud) Act 1997 gave strong power including data sharing and matching, followed by another Act in 2001 authorizing access to individuals' bank and savings accounts and utility company records, and – in some cases – to private sector payrolls. Under the 1997 Act, the Department for Work and Pensions (DWP) conducts many routine matches of personally-identifiable data, including records of housing benefit, social security, national insurance, taxation, as well as gas, electricity and telephone records. DWP proactively checks claimants' identity and dependents with other public bodies. There is also a very large data-matching exercise carried out every other year by the Audit Commission under the National Fraud Initiative (NFI). The purpose is to help detect fraudulent and excessive payments made to claimants from public funds.[115] Housing benefit fraud is still the primary problem, but the NFI is now very wide-ranging in the information it accesses. Data from local and health authorities' payroll and pensions records are used, along with records on tenants, housing benefits, social security files and information on asylum seekers. Estimates of the monetary volume of incorrect payments vary greatly, but are supposed to be in the low billions of pounds, while the results of eliminating them have been measured only in much lower amounts, estimated to have been £126 in 2004-5, including Scotland.[116] This is a tiny fraction of what is paid out in benefits, and includes overpayments, which are not fraudulent. Although fraud is fraud, questions have been raised about the proportionality, transparency and other privacy implications of data-intensive methods of plugging the hole in public expenditure.

[113] For a critical view from a computer scientist, see: Clarke, R. (2006) 'National identity cards? Bust the myth of 'security über alles'!', http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html
[114] 6 *et al.* 2005 *op cit.* n.24; Bellamy *et al.*, 2005 *op cit.* n.24.
[115] Audit Commission (nd.) *National Fraud Initiative (NFI)*, http://www.audit-commission.gov.uk/nfi/ .
[116] Audit Commission (nd.) *National Fraud Initiative 2004-5*, http://www.audit-commission.gov.uk/nfi/downloads/NFI_2004-05Summary.pdf .

10.4.4. A recent Home Office consultation paper,[117] seeks further powers against organised and financial crime, complaining that 'data sharing with other parts of the public sector is highly patchy, while sharing across the public-private divide is rarely even attempted'.[118] It calls for an improvement in these flows of information, including – with regard to Suspicious Activity Reports – matching data between the new Serious Organised Crime Agency (SOCA) and the databases of a host of government bodies, including Her Majesty's Revenue and Customs, the Driver and Vehicle Licensing Agency, DWP, and the Passport Service. There are now new initiatives including the new Ministerial Committee on Data-Sharing, MISC 31,[119] with a remit to 'develop the Government's strategy on data-sharing across the public sector'.

10.4.5. As we have seen, the police with a host of new databases recording details of citizens and offenders, and to ensure that information is shared between all the agencies involved in delivering the Government's crime reduction programme. The effect of the massive investment in IT systems and software across the criminal justice system has been to allow for the integration and cross referencing of disparate databases held across police and criminal justice agencies. In effect this means there is now one 'master' file. For instance a vehicle passes under an ANPR system, its plate number is extracted, this is then checked against the DVLC register of licensed vehicles and their registered keepers. With this information, it is then potentially possible to access all the other databases available on the PNC, for instance the database of fingerprints, criminal history, or violent and sex offenders register, and insurance and MOT databases. The extent of this integration is illustrated by Hertfordshire Constabulary's ANPR system which accesses 40 nationally or locally held databases when tracking a vehicle[120].

10.4.6. However, information sharing goes further. With the advent of multi-agency approaches to reducing the risk of crime and re-offending, the boundaries between criminal justice information and the information held by others are considerably blurred. For instance youth offending teams consist of representatives from police, probation Service, social services, health, education, drugs and alcohol misuse services and housing officers and if they have all signed an information sharing protocol, they may exchange information on individuals and families under their jurisdiction.[121] Similarly, the Identification Referral and Tracking System, developed in response to the recommendation of the Climbié Inquiry, created an information hub which alerted practitioners to all the information held by the entire range of children's services including police and youth offending teams.[122]

10.4.7. It works across national borders too. For example, new ID systems are subject to globalising forces as governments seek to 'harmonise' identification procedures; this is facilitated by the new technologies. The International Civil Aviation Organization is prominent in this, setting standards for biometric passports and, indirectly, national smart ID programs. International conventions

[117] Home Office (2006) *New Powers Against Organised and Financial Crime* (Cm 6875). London: The Stationery Office.
[118] *ibid.*: 12
[119] Cabinet Office (2006) *Ministerial Committee on Data Sharing (MISC 31)* http://www.cabinetoffice.gov.uk/secretariats/committees/misc31.asp .
[120] Hertfordshire Constabulary (2005) 'The human chassis number', Application for Tilley Award, http://www.popcenter.org/Library/Tilley/2005/05-02.pdf .
[121] For a discussion of Youth Justice Teams, see: Newburn, T. (2004) *Crime and Criminal Justice Policy*, Harlow: Longman, 211ff.
[122] For a discussion of Climbié case, see Parton, N. (2006) *Safeguarding Childhood: Early Intervention and Surveillance in Late Modern Society*, Basingstoke: Palgrave Macmillan, Ch3.

are held to develop 'globally interoperable systems' for identification in the field of 'MRTDs' (Machine-Readable Travel Documents).[123] Whilst this does not mean information must be shared, it provides the necessary infrastructure to enable it.

10.4.8. The connections between different telecommunications corporations are potentially global. In the case of both mobile telephony and Internet provision, network operators and Internet Service Providers operate transnationally, with either subsidiary or contract organisations transmitting data between them. The challenge facing regulatory bodies therefore becomes even more complex.

10.4.9. There is an increasing general tendency in the private sector in to try to integrate the vast layers of data that comprise most of the value in consumer surveillance, with many companies actively seeking to enlarge their current databases. Some firms have developed mutual use policies with other companies. Partners within coalition programmes such as those found in loyalty marketing often have agreements for some sharing of data, usually through the main coalition partner, but there is also a trend toward the creation of data cooperatives in which members share pooled sets of data. The Nectar card operated by Loyalty Management UK has over 50% of the UK population holding one of their loyalty cards. 216 catalogue companies in the UK are signed up to the Abacus data-sharing consortium, with information on 26 million individual consumers enhanced by Claritas' Lifestyle Universe. This overlays income, lifestyle, and life stage data at an individual level for each of these customers.[124]

10.5. *The Blurring of Public / Private Boundaries*

10.5.1. However, whilst both public sector and private sector share information, there are also increasingly blurred boundaries between state and private sector interests, as more and more tasks of government are carried out through a sometimes complex combination of public, private, voluntary-sector and market mechanisms, and sometimes by only one of these types. Increasingly, a variety of local partnership arrangements bring together a variety of agencies and professions so that their skills can be better focused on providing services to individuals in a more integrated way.[125] Where state information is available for private use, as has been suggested with the National Identity Register (NIR), concerns have to be raised about the limits to the consent of people as citizens and as consumers, and where those boundaries lie.

10.5.2. Direct privatisation can sometimes be the key to increased surveillance. Telecommunications is a key case in point: alongside the diversification and convergence of both technologies and functionalities in telecommunications, the diversification of telecommunications markets have vastly extended surveillance. The early 1980s saw the creation of British Telecommunications (BT) as a separate entity, its almost immediate privatisation, the opening up of market competition in the telecommunications industry, and the creation of the Office of Telecommunications as the industry regulator. The fragmentation of organisational responsibilities has meant that the range of organisations potentially retaining and mining telecommunications data has risen exponentially.

[123] See: ICAO (2003) *MRTD: Machine Readable Travel Documents,* http://www.icao.int/mrtd/Home/Index.cfm .
[124] Evans, M. (2005) 'The data-informed marketing model and its social responsibility.' in Lace, S (2005) *op cit.,* n.6.
[125] 6 *et al.* 2005 *op cit.* n.24; Bellamy *et al.*, 2005 *op cit.* n.24.

10.5.3. Even border surveillance practices are being privatised. The evidence is that the outsourcing of state border security to private commercial companies – IT multinationals, major weapons and military hardware manufacturers, consultants, risk analysts, banks, identity management and biometrics corporations – is a burgeoning practice. For example, in 2004, IBM won a £15 million contract for 'Project Semaphore', the first phase of the UK government's e-Borders programme. Project Semaphore, in a similar programme to USVISIT will integrate databases on airline passengers entering and leaving the UK. Together with 'Project Iris', also trialled by IBM, the programme will link biometric data to integrated databases that can identify anomalous patterns of behaviour. IBM is one example of a vast array of companies who now have a designated 'homeland security practice' offering data management, biometric and identity services to governments. Other notable players are: Accenture, which leads the $10 Billion US Smart Borders Alliance in the US; Oracle, whose ubiquitous identity management systems are now being used by the UK and US as 'homeland security solutions'; and consumer electronics and telecoms companies such as Ericsson, who are contractors for the US Strategic Border Initiative (SBI).

10.5.4. In many instances the biometric border schemes are linked to frequent flier programmes of other loyalty cards and, in the US, the trend is toward corporate sponsorship by credit providers such as Mastercard. The expansion of privatized 'ID guarantee' has the potential to render obsolete some of the debates about national ID cards and biometric passports.

10.5.5. There is also an apparent move to incorporate citizen groups and watch groups into border surveillance practices. This is in its most advanced for in the US, where programmes such as Highway Watch, Citizen corps, Coast Watch and River Watch train citizens to 'look out for unusual activities'. However, there is one element of this form of everyday surveillance that has particular resonance in the border surveillance domain. For many of the private companies bidding for, or awarded, border surveillance contracts, consumer electronics such as mobile phones, PDAs and palm tops have played a central role. IBM, for example, contracted for the UK e-borders system, also sponsored the US homeland security citizenship programme that allowed for personal computers, mobile telephones and consumer electronics to digitally connect neighbourhood security to homeland security.

10.5.6. Finally, states can seek to dominate or subvert international or private organisations that supply information products or which regulate information infrastructure. The American NSA has established a working relationship with most of the major U.S. software and hardware companies, and through these relationships has ensured that encryption systems within export versions of software in particular are less sophisticated than US internal market versions, and are more easily crackable. The NSA and GCHQ also do deals with International Licensed Cable (ILC) companies to allow interception. The NSA in particular has been reported to have representatives on transnational standards-setting committees, in particular the MFA Forum (previously the Frame Relay Forum), an unaccountable body responsible for the development

of common standards for data transfer, and which also contains all the major telecommunications and computer companies from industrialised nations[126].

10.5.7. There is thus a multiplicity of surveillance agents and agencies often with their own databases, which are increasingly subject both to commercial pressures to purchase and sell valuable information and to state desires to accumulate information for anti-terrorist, anti-fraud and law-enforcement purposes.

11. The Social Consequences of Surveillance

11.1. We now turn more overtly to the social consequences of the surveillance technologies and processes we have summarised in the previous sections. Critiques of surveillance are most frequently framed in terms of privacy and this is undoubtedly a vital area, although we would prefer to discuss it as one aspect of individual autonomy. However we would also like to emphasise the far less frequently discussed outcomes of choice and consent; and most importantly, the sorting, categorisation and targeting processes on the life chances of individuals and whole groups or communities, their relative mobility, and access to opportunities.

11.2. *Autonomy: Anonymity and Privacy*

11.2.1. The autonomy of individual persons has multiple components, two of which we consider here to be particularly affected by surveillance. The first is anonymity. Anonymity has long seen as one of the key aspects of modern life, particularly in the city. Surveillance can certainly help to create many new services, and a speeded-up urban lifestyle characterised by individually tailored services, continuous electronic and physical interaction, an always-on digital economy, and the transcendence of many of the time and space barriers that traditionally acted to inhibit urban life. However one of the first casualties of pervasive surveillance, and particularly of ID systems, is the anonymity that allowed people to escape from the intense human surveillance strictures of small communities. In many ways, a general initial condition of anonymity allows the individual the ability to make their own identity through their actions and relationships.

11.2.2. Of the one and a half million people sentenced by the courts in 2003 some 107,000 were sentenced to immediate custody.[127] A sentence of imprisonment not only involves a loss of liberty, but also the second component of autonomy, privacy. In UK prisons, offenders all subject to almost constant surveillance. Since 1996, this surveillance regime has included mandatory drug testing with an expectation that between five and ten per cent of the prison population would be subject to a random test each month.[128] In 2004/5 a total of 51,484 tests were carried out, of which 11.6 percent were positive.[129] Even once released from prison, offenders are also increasingly subjected to electronic monitoring either as a condition of early release from prison under

[126] Seeberg, K. and Elkjær, B. (1999) 'Tele Danmark in a club with Echelon spies', *Ekstra Bladet* (Denmark), 26 September. The MFA Forum can be found at http://www.mfaforum.org/ .
[127] Home Office (2005) *Sentencing Statistics 2003: England and Wales*. London: Home Office, 3.
[128] Singleton, N. *et al.* (2005) *The Impact and Effectiveness of Mandatory Drug Testing in Prisons*, Home Office Research Findings 223, London Home Office.
[129] HMPS (Her Majesty's Prison Service) (2005) *Her Majesty's Prison Service Annual Report and Accounts*, Annex 1: Statistical Information, London: Stationery Office, 110.

the Home Detention Curfew Scheme[130] or as a condition of being released on parole.[131]

11.2.3. Another frequently relatively constrained population is that of patients. The patient's autonomy, dignity, and right to privacy has always been of significant concern. Health data are regarded as 'sensitive', although some are more sensitive than others. Many professionals worry whether traditional assumptions about confidentiality can be maintained when it comes to, for instance, making 'single shared assessments' of certain patients who are dealt with by social care as well as by health professionals, or where data on mental-health patients may require that data be shared with yet other agencies, sometimes including the police. For nearly ten years, a system of 'Caldicott Guardians', named after the author of a report that looked into the confidentiality of identifiable patient data in the NHS,[132] has been in place. This means that every NHS body has a designated person who oversees confidentiality, controls access to patient information, helps to develop protocols for information-sharing across organisations, and works to ensure good practice concerning patient data. This system is part of a wider 'information governance' framework in the NHS, and is now also being used in social care agencies. But whether or not the 'guardian' system has worked well – the results have been patchy and there are many shortcomings, owing to factors including the complexity of 'eHealth' information technologies and information flows, inadequate resources and training, and weak institutional role support[133] – controversies over the disclosure of health data have arisen in the context of anti-terrorism, crime-fighting and Audit Commission investigations. The Department of Health has formed a confidentiality strategy and a code of privacy and confidentiality practice,[134] and the Information Commissioner has produced guidance for the health sector when anxiety developed over the sharing of NHS data with other agencies.[135]

11.2.4. Privacy questions are also endemic to workplace surveillance. When discussing privacy issues in this domain, it is important to focus on the full range of privacy concepts: privacy and the human body, privacy in social relations, and privacy and personal space as well as information privacy[136]. It is also important to consider fully the implications of disclosure: whether the employee had given their authority for boundaries relating to their body, social relationships, personal space and information to be crossed; and whether they were aware of who was going to be party to that information.[137]

11.2.5. Drug tests, in particular, can deter many from applying for jobs where they are likely to be tested. The tests do not distinguish between heavy and

[130] The HDC scheme allows for those sentenced to between 3 months but under four years imprisonment to be released between 2 weeks and four and a half months early on a curfew enforced by electronic monitoring. In 2004/5 19096 people were release early under the scheme. See: NPS (2006) *op cit.* n. 82.
[131] *ibid.*
[132] Department of Health (1997) *Report on the Review of Patient Identifiable Information* (The Caldicott Report). London: Department of Health.
[133] NHS Scotland (2004) *A Review of the Work of the Caldicott Guardians*, http://www.confidentiality.scot.nhs.uk/publications/Caldicott%20Review.pdf .
[134] Department of Health (2001) *Building the Information Core: Protecting and Using Confidential Patient Information.* London: Department of Health; Department of Health (2003) *Confidentiality: NHS Code of Practice.* London: Department of Health.
[135] Office of the Information Commissioner (2002) *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998.* Wilmslow: Office of the Information Commissioner.
[136] Laurent, C. and Privacy International (2003) *Privacy and Human Rights 2003. An International Survey of Privacy Laws and Developments*, Washington DC / London: Electronic Privacy Information Centre (EPIC) / Privacy International. http://www.privacyinternational.org/survey/phr2003/ .
[137] Ball, K. (2001) 'Situating workplace surveillance: ethics and computer based performance monitoring', *Ethics and Information Technology*, 3(3): 211-223.

recreational drug users and abstinence a few days before the test will usually yield a negative result.[138] Employers' capacity to record and store employee communications also raises privacy concerns, first because private conversations may contain confidential information (e.g. a credit card number), second because this information may be stored on offshore servers which fall under different jurisdictions, and third because of the relative coverage and broadcast of relevant policy. Appropriate policy is difficult to define in respect of covert surveillance. There is some debate as to whether organisations are required to provide a general notice to staff that they may be subject to it, or whether this can be avoided altogether. The collection of employees' personal information and other information about their lives can compromise privacy if employees do not authorise the disclosure of their information and it is broadcast to unknown third parties.[139]

11.2.6. In this context, we must also return to the proposed national ID system. A recent House of Commons Select Committee report[140] has complained about the disturbingly unclear range of proposed functions of ID cards. This remains the most controversial British issue involving potential threats to privacy through the surveillance involved in the establishment and use of the NIR created under the Identity Cards Act 2006. While ID cards will serve traditional Home Office functions regarding law enforcement (broadly speaking), immigration and asylum, national security and counter-terrorism, they are also intended to 'secure the efficient and effective provision of public services' in ways that still sketchy, but that potentially involve a large array of departments and agencies which relate to specific service fields. A key element is the provision of a unique reference number for each person, facilitating the integration of a vast number of data sources. Moreover, indications that government foresees interaction between the public and private sectors in the use of the ID card, including access to the NIR, adds further concerns about limitations and privacy safeguards for this potential extension of surveillance.

11.2.7. Although data protection and privacy laws[141] were developed to limit such activities, these have found it very hard to keep pace with technical change or the ingenuity of those trying to sidestep regulation. If the UK ID card system is, as advertised, to guard against 'identity theft,' then this suggests that commercial data relating to banks and credit cards will be accessible as well as those relating to government departments such as immigration or health.

11.2.8. For privacy regulators there is an increased pressure on limiting the uses to which personal data can be put, the length of time it can be stored and so on. The use of everyday consumer telecommunications electronics to convey data, information or images from private domains to the sphere of public authorities blurs the boundaries between public and private spheres. As the ACLU have commented in their study of a new surveillance network, businesses and citizens are being 'conscripted into the construction of a surveillance society'.[142]

11.2.9. Consumer surveillance, although frequently entered into because of a voluntary decision (to buy or not) also has significant privacy implications

[138] Drug tests merely indicate the presence of various recreational drugs. Commentators refer to them as 'intelligence tests': to fail one the candidate would need to be very stupid!
[139] For more on email monitoring, see: Lloyd, J. (2006) 'Management email monitoring brings Big Brother to mind'. *Receivables Report for Americas Health Care Financial Managers* 21(1): 6-7
[140] House of Commons Science and Technology Committee (2006) *Sixth Report*, HC 1032, London: The Stationary Office.
[141] See e.g.: UK 'Data Protection Act' 1998, http://www.opsi.gov.uk/acts/acts1998/19980029.htm
[142] Stanley, J. (2004) *The Surveillance-Industrial Complex*, Washington DC: ACLU.
http://www.aclu.org/FilesPDFs/surveillance_report.pdf

suggesting that the breadth and depth to which consumer surveillance may go should be limited. Privacy legislation within the European Union and in countries that have enacted similar omnibus legislation stipulating limitations on the collection and use of personal data, require both that purposes be specified and security safeguards remain in place for personal data. Two of the data protection practices included in the legislation are incompatible with the data mining techniques that underlie consumer surveillance. First, the use of data cannot be clearly specified to the consumer. It is impossible to predict the results of data analysis conducted with technology designed to discover non-obvious relationships and patterns within sets of data. This means that companies are unable to inform customers fully as to the use of their data, as the categories produced by data analysis are emergent. Second, because the principle of limiting the use of information defeats the very purpose for the collection and use of consumer data. The increase in data and potential variables increase the system's predictive accuracy.[143] Beyond the issues with these prinicpals even though privacy legislation limits the use of *personally identifiable* information, information stripped of these identifiers can continue to be used for consumer surveillance practices. This in turn can have the same effects for those categories of high-risk consumers.

11.2.10. Of particular interest in mobile telecommunications is the differentiation between the storage and monitoring of 'transmission' information, necessary for communications to take place (largely generated automatically), and 'personal' information such as name, address and payment details, thereby falling under the auspices of relevant data protection legislation. Mobile phone network operators and service providers gather and store a wide range of data as a matter of course.

11.2.11. For state law enforcement and political policing, the distinction matters less. The Regulation of Investigatory Powers Act (2000) made traffic and billing data available on request to UK law enforcement organisations. Under RIPA, a senior officer is required to ask a telecommunications operator for traffic data. The Interception Commissioner may exercise oversight after the fact on data requests, but the investigating officer in any case need only justify the request to a senior officer. By the end of 2002, the BBC was reporting that law enforcement bodies had made over 400,000 requests for traffic data from mobile network operators.[144] For the law enforcement community, any claims that the mobile handset has no relationship to the user, and that the collation and processing of pseudonymised traffic data has no data protection implications, appears to be inoperative.

11.2.12. While privacy legislation does mitigate some of the concerns inherent in consumer surveillance, its individualised focus and the hidden information processing techniques means that social categories and their effects are concealed from those directly affected by them. Genuine informational control requires an increase in organisational transparency regarding data gathering and information processing as well as clear indications of when the security of personal data has been breached. The difficulty is in reconciling this transparency with the demands of a highly competitive economy in which transparency may in fact undermine the advantages gained through an organisation's data processing. Without finding this balance, whether through regulatory regimes or ethically transparent corporate practices, the concern

[143] For an extensive discussion of these issues with FIPs, see: Tavani (1999) *op cit.* n.60.
[144] See n.80.

remains that consumer surveillance will continue to perpetuate and amplify social divides and sorting that is antithetical to democratic principles. Consumer surveillance then stands to increase as a 'cybernetic triage' separating consumers based on their presumed economic and political value rather than on their initiative and self-determination.[145]

11.3. *Choice and Consent*

11.3.1. The next area is that of choice and consent. Choice has played a major role in the debates about surveillance and data protection in North America. Yet in the United Kingdom, it has had a somewhat lower profile in contrast other means of protection.

11.3.2. In medicine, there are several forms of consent: consent to treatment; consent for information transfer; and consent for personal medical information to be used for medical research. The key question in all cases is what information has been provided to allow the individual to make that decision. 'Informed patient consent' to the use of personal data is required not least since the gross abuses of medical science ethics perpetrated in the WWII concentration camps. When patients are requested to release information into large research databases, one has to ask whether all potential usages of data over time can be foreseen, and whether new consent might be necessary in future. As a consequence, there is often the additional requirement that data collected for medical (including medical research) purposes only be used for the specific purpose for which it was originally acquired. Any new purpose then requires new information and a new signed consent form from each included patient.

11.3.3. This may seem then to be a clear example of the problem of choice and consent in surveillance: can one chose whether or not to be surveilled if one wants to live a normal life? How is it possible anymore to argue that we have consented to surveillance? The issue of consent can be seen at work throughout the criminal justice system. We do not consent to CCTV system monitoring us as we walk though public space, and no one has consented to having their vehicle movements logged at the ACPO's ANPR Centre. Arrestees do not consent, and are coerced, into providing fingerprint and DNA samples, which will be permanently logged on the police national database, even if they are released without charge. And, while a person cannot be forced to give a urine sample to test for the presence of drugs, it is hardly a matter of choice, as refusal can result in a fine, imprisonment or both. It is almost impossible for a person to know how information is being used, and how it may, in subtle ways, affect their lives; for instance, by increasing the chances that their vehicle is stopped by the police, or the demand that they pay in advance for goods and services.

11.3.4. One answer might be to make state surveillance interactions with citizens non-compulsory where this is possible, which is what has been proposed with ID in Britain. However, this is largely an illusory answer, for once it is needed for a range of service-access it will become *de facto* compulsory. Moreover, existing identifiers relate to single roles, as drivers, consumers or tourists whereas the ID card system gives the government powers to monitor activities across a range of roles that include all of these as well as that of citizen.

[145] This is what is understood as 'the panoptic sort' described in detail in: Gandy (1993) *op cit.* n. 24.

11.3.5. In the workplace, issues of consent are also not simple. There is debate and differing attitudes across nations as to whether organisations are required to provide a general notice to staff that they may be subject to covert surveillance, or whether this can be avoided altogether. In Australia, for example, employers are required to get permission from a magistrate to conduct covert surveillance on employees from a magistrate. In the UK, under the Regulation of Investigatory Powers Act (RIPA) 2000, if the business is protecting a 'legitimate interest' it can covertly intercept employee communications, although it does have to comply with Data Protection Act requirements too. In the case of mystery shopping, for example, opinion is split between those who argue that the practice is unethical because of the levels of deceit, compromise and the lack of consent involved.[146] Others argue that employers need to present the results of mystery shopping to staff, to raise awareness of it in a way which will not compromise the research.[147]

11.4. *Discrimination: Speed, Access and Social Exclusion*

11.4.1. Discrimination, in the form of differential speed, ease of access and various degrees of social exclusion is a major outcome of the social sorting processes produced by surveillance. The old bureaucratic logic of government administration now works its way through both biometrics and networked identification systems, into a world fraught with subtle identities and identifications. In this world those with access to resources are highly mobile – international businesspersons, tourists and the like – and their identification systems (from credit cards to frequent flyer cards) tend to accelerate ease of movement. But for others, who are working (or worse, unemployed) migrants, refugees or asylum seekers, not to mention those with distinctive 'Muslim' or 'Arab' names, these systems tend to militate against movement both within and between countries.

11.4.2. Governmental logic has changed. While older, twentieth century understandings of citizenship stressed the *inclusion* of all eligible persons in systems of health, welfare and legal protection, newer citizenship practices, including ID systems, seem to stress *exclusion* of undesirable elements.[148] Key events, starting symbolically (though not historically) with 9/11 have catalysed rapid growth of new surveillance and identification systems.[149] The difficulty is that many people are on the move, for many reasons and that ID systems are sought that classify them according not only to citizenship but also to status – temporary, permanent, national and so on. Searchable databases already facilitate such social classification and categorisation.

11.4.3. The intensified surveillance of urban life also involves powerful processes of social exclusion. This is characterised by the creation of disconnections for those people and places deemed in some way unprofitable or risky. Crucially, then, the new surveillance technologies can thus forcibly *slow down* certain people's lives, making them logistically more, not less, difficult. Much of this social sorting by surveillance systems now works automatically (i.e. without human discretion), continually (i.e. 24 hours a day), and in real time (i.e. without delay) through software. Very often, the motivation is

[146] Shing, M.N.K. and Spence, L (2002) 'The limits of competitive intelligence: is mystery shopping ethical?' *Business Ethics: A European Review* 11(4):343-353.
[147] Wilson, A.M. (2001) .Mystery shopping: using deception to measure service performance,' *Psychology and Marketing* 18(7); 721-734.
[148] Bigo, D. (2004) 'Globalized in-security: the field of the professionals of unease management and the ban-opticon,' *Traces*, 4.
[149] Lyon, D. (2003) *op cit.* n6; Ball, K. and Webster, F. (eds.) *The Intensification of Surveillance*, London: Pluto Press.

overcoming the barriers of electronic and physical congestion facing affluent, privileged or powerful people and places, as they confront the challenges of living and operating in dense, urban, and increasingly mobile societies which place a premium on networked connections and flows connecting to other places.[150] However once introduced, both access and blockage are increasingly policed automatically,[151] threatening a technological lock-in dividing contemporary societies more decisively into high-speed, high-mobility and connected and low-speed, low-mobility and disconnected classes.

11.4.4. This can work itself deep into the very infrastructure of society. We have seen how expedited border crossing can speed up the journeys of paid-up members of frequent flyer programmes. In cities, commercial judgements, based on continuous connections to credit registers and the like, could lead to the regular exclusion and targeting of people deemed to be commercially marginal within increasingly commercialised and gentrified town and city centres. Algorithmic CCTV systems may embed social prejudice deep into the very software that makes them work. With the discretion of camera operators increasingly removed, the code within the software that 'decides' which behaviours, appearances, faces and identifiers warrant further action, scrutiny, or exclusion, out of the mass of a city's or nation's population, becomes the key site for regulation. ID systems may also subtly classify populations according to opaque criteria that skew the system against those already likely to be disadvantaged. Such social sorting tends to produce second-class citizenship. When cultural and national identity has become such a contested dimension of life, carrying a heavy freight of life-chances and choices, memories and hopes, it is ironic that parallel efforts are made to reduce it to machine-readable formulae and algorithms for ease of bureaucratic, policing and corporate administration.

11.4.5. Exclusion is even found in the pricing structures for goods. With Amazon.com already shown to be selling DVDs to different customers at different prices, the question is raised whether regulatory intervention might be necessary to ensure that mass commercial price-fixing does not emerge, for example, based on the operation of automated RFID surveillance. Consumers have become increasingly vulnerable within the personal information economy. The tremendous reliance on particular technologies and unique numbers or codes to indicate identity creates opportunities for informational abuse and exploitation. Continuing innovations in data processing and increased collections of different types of data lead to social sorting practices rife with concerns for discrimination and exclusion.

11.4.6. Whilst it is difficult to draw conclusions about workplace surveillance and social exclusion, mainly because of the pre-existing occupational and social structural determinants of labour markets, one area of workplace surveillance is beginning to stratify opportunities for employment: e-recruitment. Sifting through large volumes of CVs and searching for potential candidates raises the question of discrimination in two ways. First, e-recruitment is subject to biases and 'rules of thumb' similar to those currently used by recruiters when they face complex choices between a range of candidates.[152] Keyword searches are now routinely being used as selection tools, and as the use of particular keywords

[150] Andrejevic, M. (2003) 'Monitored mobility in the era of mass customization,' *Space and Culture*, 6: 132-150.
[151] Lianos, M. (2001) *op cit* . n.109; Lianos, M. (2003) 'Social control after Foucault,' *Surveillance & Society* 1(3): 412-430. http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf .
[152] Tversky, A. and Kahneman, D (1974) 'Judgement under uncertainty: heuristics and biases,' *Science* 185(4157): 1124-1131

varies between recruiters, it may yield different results.[153] Whilst it may be argued that eliciting the right results with particular keywords is indicative of the professional expertise and tacit knowledge of the recruiter, it may also reflect their own biases. Further complexity arises when one considers that CV writing skills vary so much between candidates. The use of standard forms goes some way to remedy this problem, as well as the use of multiple words to search for a qualification, as well as tight policy regulation of the practice.

11.4.7. Second, it is discriminatory in the sense that certain social, economic and ethnic groups do not have easy access to the internet. Hence a concentration on e-recruiting effectively excludes these groups from the labour market altogether. Whilst many niche websites have now developed, initially its use was directed towards white, male middle class occupations in IT and engineering.[154] There is a strong temptation for companies to standardise and formalise e-recruitment processes which will yield 'more of the same' rather than a diverse set of applicants. Indeed Marconi Capital revised its e-recruitment strategy when they found that it did not attract the ethnic or social mix of people they wanted and it has also been reported that women were more likely to deselect themselves from online recruitment processes because of its impersonal nature.[155] The UK disability rights commission investigated 1000 websites and found that 81% failed to satisfy the most basic web accessibility guidelines, which means that eight out of ten websites in the UK exclude 1.3 million people of working age applying for jobs online.[156] Explicitly using varied recruitment channels, advertising on diversity websites, and reflecting diversity requirements are key steps organisations can take.

11.4.8. Ironically, as we saw in the Introduction, a great deal of surveillance is aimed at inclusion from the basic mechanisms of the welfare state onwards and this has only been increased by 'safety-first' ideology. A key example is the enormous development of policy to safeguard children in a comprehensive and precautionary manner. This involves efforts to combat social exclusion and to deal with young offenders, and, especially, interventions in the education sector. It includes new departures such as the children's database, or 'information sharing index' for 150 local areas, that will include data on all children in England and Wales up to the age of 18 years. The purpose is wider than child protection, and is aimed at a more holistic purpose relating to children's welfare and the provision of services: the indexes will identify each child and show whether they are receiving the relevant services. The database is to include basic details plus unique identifying numbers and contact details for parents, schools, health carers and other professionals who supply additional needs and who may have important information or assessments to share. This idea, which featured prominently in the 2003 Green Paper, *Every Child Matters*[157] and was legislated for in the Children Act 2004, is intended not only to bolt the door against future tragedies, but also to fulfil a much wider care-agenda commitment that children's needs are being provided, thus involving the education and health services as well.

[153] Mohamed, A.A., Orife, J. and Wibowo, K. (2002) 'The legality of key word search as a personnel selection tool,' *Employee Relations* 24(5).
[154] Sharf, J. (2000) 'As if g-loaded adverse impact isn't bad enough, internet recruiters can be expected to be accused of 'e-loaded' impact,' *The Industrial-Organizational Psychologist* 38:156.
[155] Smethurst, S. (2004) 'The allure of online,' *People Management* 10(15): 38 – 40; Czerny, A. (2004) 'Log on turn off for women,' *People Management* 10(15): 10.
[156] Smethurst (2004) *op cit.*
[157] Chief Secretary to the Treasury (2003) *Every Child Matters* (Cm 5860), London: The Stationary Office. http://www.everychildmatters.gov.uk/_files/EBE7EEAC90382663E0D5BBF24C99A7AC.pdf .

11.5. *Democracy, Accountability and Transparency*

11.5.1. There are many questions here: what are the limits of public scrutiny? How is the boundary between commercial databases and public and state security to be regulated? How are private companies to be made accountable for errors and false hits in their database systems? For example, currently there is extremely limited access for citizens who find themselves on a 'smart border' watch list. While multiple agencies and authorities can access the system or place information on the system, there is restricted capacity to remove or correct data. Finally, there are substantial questions surrounding the accountability of elected governments to their citizens and the 'offshore' nature of many of the private contractors of contemporary surveillance systems. In effect, commercial banks of data such as credit card transactions or mobile phone records that are held by multinational corporations can be 'offshore' and beyond the direct reach of a political jurisdiction. Recent examples of multinationals extraditing information will raise specific challenges for public scrutiny and regulation, particularly when a company holds the commercial data *and* has a contract for surveillance functions.

11.5.2. Appropriate policy is especially difficult to define in respect of covert surveillance. Where this involves transnational espionage, as with the ECHELON system, the fact that for official purposes such systems do not 'exist' or are held to be in a realm beyond the law, or conducted in partnership with the agencies of other states, makes a mockery of ideas of choice and consent. The UK has a long tradition of secrecy and a blanket assumption of exemption on behalf of the intelligence services. For example, the Intelligence Services Act (ISA) 1994 specifically allowed GCHQ 'to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material' for a wide range of purposes 'in the interests of national security […] the economic well-being of the United Kingdom [or] in support of the prevention or detection of serious crime'[158].

11.5.3. It is commonly believed that a warrant is required for every specific instance of telecommunications interception ('telephone tapping'). This is true of ordinary police surveillance. However, the ISA actually stated in a particularly cunningly-worded paragraph that 'No entry on or interference with property or with wireless communications shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section'[159], which does not say that any of the actions mentioned is unlawful *unless* authorised by a warrant. Within the meaning of the Act 'entry on or interference with property or with wireless telegraphy' could be carried out lawfully without a warrant.

11.5.4. Sometimes, in other nations, surveillance and particularly state information sharing has been severely criticized by regulators and media. Perhaps the most notable instance of this was the Canadian Government's Longitudinal Labour Force File, which linked a vast amount of federal and provincial administrative data on Canadian citizens, including information about social assistance, income tax, immigration, employment services, and unemployment insurance. As many as 2,000 pieces of information on about 34 million Canadians were involved in this surreptitious, weakly regulated, public-

[158] Intelligence Services Act 1994, Chapter 13, Section 3, London: HMSO.
[159] Intelligence Services Act 1994, Chapter 13, Section 5, London: HMSO..

service-related research programme. Following its exposure, public outcry, and strong action from the federal Privacy Commissioner, it was dismantled in 2000 with the requirement that much more stringent privacy protection, including encryption and 'disidentification', as well as stronger accountability and transparency, be incorporated into any such future sharing of information.[160] In Japan in 2002, a major scandal emerged when it came to light that the Defence Agency had been compiling secret files on those requesting information about them, and that the Self-Defence Forces were systematically collecting data on individuals who made information-disclosure requests, including occupation, workplace, and possible connections with SDF workers[161].

11.5.5. Under legislation in many countries, citizens have a right to know what information is held about them, and how it is being used, although there are exceptions to this requirement. This right requires a 'data controller' to provide to each individual information on all the data they hold on her and details of any processing it has been subject to. This goes some way to rectifying the asymmetry of power of the surveillance gaze, particularly where consent to use our personal data has been implied, rather than positively granted. However, large numbers of people do not know their rights, fail to exercise them, and receive little help from others in doing so.

11.5.6. Intensified dataveillance is becoming a normal feature in the modern state, and may, in itself, be justifiable – and justified by those who promote them – in the public interest. These activities may often be explicitly empowered by parliament. What makes them problematic is their manipulation of large quantities of personal data in ways that may overstep the mark established by data protection principles and laws (parliament, once again), and by other constraints and guidelines about how information is to be collected, collated and communicated. We may become accustomed to being surveilled, our activities and movements tracked and also anticipated, without noticing it, and – especially in the public services – without the ability to opt in or opt out, or to understand fully what happens to our data. We may well accept as 'reasonable' the limitations on privacy that we might otherwise reject if we were to consider what being a citizen should mean. It is far from certain that the political situation will, at the end of the day, allow privacy rights to stand up strongly to the claims of government organisations made in the 'public interest', even if the public interest seems clear and of greater importance. If surveillance is meant to be 'proportionate', a lot depends on how that terms is interpreted, and on who interprets it. A lot also depends on the safeguards that surround the new, intrusive developments.

11.5.7. However, in promoting new plans and programmes, government has also, from time to time, recognised the question of privacy and the dangers of surveillance. It has therefore attempted to bring to the surface the important question of public trust in the information processes of 'information age government', including public-service provision both online and in other ways. Sometimes the 'down-side' has not been considered in anything like the depth that the presumed benefits have been. But privacy issues have been important in the debates about trust, although not so prominent or so influential as was hoped for by those who have been worried about the surveillance potential of the new,

[160] Todd, D. (2001) *Politicizing Privacy: 'Focusing Events' and the Dynamics of Conflict.* Unpublished Master's Thesis, University of Victoria, BC, Canada, 58-86; see also: HRDC Canada (2000) 'HRDC dismantles longitudinal labour force file databank', 29 May, http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml .
[161] Abe, K. (2004) 'Everyday policing in Japan: surveillance, media, government and public opinion,' *International Sociology*, 19: 215-231.

more integrated and extensive, use of databases and like. When the Performance and Innovation Unit produced its report in 2002 on privacy and data-sharing,[162] it went further towards trying to provide solutions that would both enable personal data to be used and shared, and that would also enhance the protection of privacy. However, putting its recommendations into practice has, for the most part, fallen behind, overtaken by events and new initiatives which have made the prospects of good privacy protection in the public services look more remote unless countervailing safeguards can be built into these initiatives, or applied to them afterwards.

[162] Cabinet Office Performance and Innovation Unit (PIU) (2002) *Privacy and Data-Sharing: The Way Forward for Public Services*. London: Cabinet Office.

Part C/1: A Week of Life in the Surveillance Society, 2006

12. Introduction

12.1. It is London in 2006. The Jones family are returning from their holiday in Florida. Dad, Gareth is a manager in a call centre, and mum Yasmin is a social worker. Yasmin is originally from Pakistan and holds dual nationality. Her mum, Geeta, who holds a Pakistani passport is with them too, as are their three children, 18 year old Ben, 14 year old Sara and 10 year old Toby.

12.2. The Jones family are citizens in the surveillance society. Throughout the week following their return, sometimes unwittingly, and sometimes with complete awareness, their lives interact with and are shaped by surveillance systems. In the following pages we show how their everyday activities are now embedded within surveillance systems, and how surveillance affects their actions and relationships.

13. At the Airport

13.1. Although it is the end of the family holiday and they are heading home Gareth Jones is feeling pleased with himself. This was his treat. As regional manager for 'Sentasi' Britain's fasting growing call centre network, he had landed a sizable performance bonus for his part in setting up new offices in Hyderabad[163]. It was his working knowledge of Urdu that made the difference, acquired from his twenty-two year marriage to Yasmin. The bonus had afforded the holiday of a lifetime: three weeks in Florida, Walt Disney World, the Keys, and whale watching. With Ben now off to university next year (provided he achieved a better grade in one of his A levels which he was retaking part time at school), this might have been the last complete family holiday. And Yasmin had really needed the break. Once Toby, their last child, had started school, she had trained as a social worker, passed with flying colours, and was immediately offered a job in a multi-agency youth offending team. It had been four years since their last proper holiday. And he was really pleased that Yasmin's mother, Geeta had joined them; it was a small 'thank you' for the financial help she had given them over recent years. He was also pleased because Geeta and Sara had that special bond, as grandmother and granddaughter often had, which helped to calm her somewhat volatile teenage temper. And he was finding it increasingly difficult to relate to her. He knew she had been skipping school and he blamed the crowd she was mixing with; she called them 'Goths'. He called it morbid: all dressed in black, hair dyed black, studded boots, and piercings all over the place. He had made her remove the one in her tongue but had eventually given in to the multiple ear studs. Teenagers!

13.2. As he waits in line he hopes that they would not face the same problems in boarding the plane as they had when they left from Gatwick. As they had passed through security the whole family had been taken to one side, their hand luggage not

[163] All names of private individuals and companies in the text are fictional. Real world analogues are footnoted.

only x-rayed, but also thoroughly hand searched, and they had all been questioned at length about their recent international travel. It had taken over half an hour before they had been allowed to proceed. They had been told they were singled out at random, as part of the additional security measures now in place. But he suspected it had been because his wife and mother-in-law held Pakistani passports.[164]

13.3. He is wondering whether the same thing will happen on their way back. As he places his hand luggage on the conveyor belt along with his keys, loose change, jacket and shoes in the basket, walks though the body scanner he is relieved that he doesn't trigger an alarm. But in the adjacent aisle where the women had been directed, he watches with some embarrassment as his daughter removes her boots, neck choker, big black belt, and studded jacket and, even in this state of relative undress, still triggers the buzzer as passed through the scanner. She is made to pass through again and, as the alarm sounds once more, she is waved aside to a small curtained cubicle where she is subjected to a thorough body search by a female security guard before being allowed to proceed. Once through security they are forced to wait in line again to be photographed and fingerprinted, as they had been when they had entered the US three weeks before[165].

13.4. The rest of the procedures are uneventful, immigration goes without a hitch, with Yasmin and Geeta only taking a few minutes longer to clear the non-EU/UK passport holders desk, and baggage reclaim is efficient.[166] But Ben and Toby have stacked a trolley high with their cases, and as Ben turns a corner, the cases topple off, crashing into Geeta, who is knocked to the ground. As Yasmin and Ben check to see if she was alright, two members of airport staff appear almost immediately[167] and most helpfully organise for an electric passenger cart to come and take them and their luggage to their courtesy bus which will drop them at the car park.

---

[164] He is partly right about this. However the actual reason for the stop is that they had been subject to 'passenger profiling'. In this case the fact Mr Jones booked his holiday at the last minute, has a recent history of travelling to Pakistan, that two members of the party have Pakistani passports and that they requested not to sit together (the children all wanted window seats) flagged them as high risk passengers needing addional security checks. The profiling was part of a trial for *Project Semaphore*, which was introduced as part of the UK Government's e-borders programme, at selected airports from 2004. Initially it targeted six million passengers a year on a number of international air routes to and from the UK. It uses on-line technology and advance passenger information provided by airlines, to custom police and immigration officials before arrival to screen and record individuals as the enter and exit the UK, providing a comprehensive passenger movement audit trail which can be checked against other databases. See: Home Office (2004) 'Cutting-edge technology to secure UK borders,' 28 September, http://press.homeoffice.gov.uk/press-releases/Cutting-Edge_Technology_To_Secur?version=1 . In January 2006 it was announced that the this would be extended to all cover the 40 million domestic journey made by plane or ferry: Travis, A. (2006) 'Security services and police to get UK air passenger details in advance,' *The Guardian* 24 January, http://www.guardian.co.uk/airlines/story/0,,1693586,00.html .

[165] In the wake of September 11 2001, the US introduced biometric identification for foreign visitors to the USA. Since 2004 under the USVISIT programme this has meant that on entry and exit, a U.S. Customs and Border Protection Officer reviews your travel documents, such as a visa and passport, questions you about your stay in the U.S and then uses an inkless, digital fingerscanner to capture the fingerprints of left and right index fingers. The officer also takes a digital photograph of the passengers face. The biometric identifiers are used to confirm the passenger's identity so that their details can be checked against a variety of data bases including Arrival Departure Information System (ADIS), which stores traveller arrival and departure information; Advance Passenger Information System (APIS), which contains arrival and departure manifest information; Computer Linked Application Information Management System 3 (CLAIMS 3), which holds information on foreign nationals who request benefits; Interagency Border Inspection System (IBIS), which maintains "lookout" data. IBIS in turn interfaces with the Interpol and National Crime Information Center (NCIC) databases; Automated Biometric Identification System (IDENT), which stores biometric data of foreign visitors; Student Exchange Visitor Information System (SEVIS), a system containing information on foreign students in the United States; Consular Consolidated Database (CCD), which includes information about whether an individual holds a valid visa or has previously applied for a visa. See EPIC (2006) 'United States Visitor and Immigrant Status Indicator Technology (US-VISIT),' http://www.epic.org/privacy/us-visit/ . See also: Deparment of Homeland Security (nd.) 'US-VISIT Multilingual Videos and Brochures,' http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0435.xml .

[166] Aided in part by the bar code tagging of their suitcases that helps the airline keep an online database of all baggage movements and destinations.

[167] They are alerted by radio from the Central CCTV monitoring system, which picked the incident up on their screens.

14. Shopping

14.1. As Yasmin drives out of the airport, she switches on the Sat Nav system, which will guide them home by the most direct route, but also alert them to the presence of speed and red light cameras on the way. Yasmin knows she doesn't need to be reminded of the speed limit but Gareth wouldn't be without sat nav. He already has six points on his licence for speeding offences and a further six would see him banned for a year, something he can ill afford in his line of work which requires so much driving.[168]

14.2. On the way back they agree to stop off at a massive out-of-town shopping mall. Gareth and Yasmin decide to go to the nearby supermarket, NSC, to do a quick shop for dinner that night, while the kids go to 'Denim Warehouse' which has a sale. Yasmin will get the family's weekly groceries on Monday evening after work. At 'Denim Warehouse', Ben buys some new jeans, impressed with the free baseball cap that came with them, which he puts on Toby's head as they leave the store. He is less impressed when, as they are sitting on a bench with Sarah whose met some other 'Goth' kids, two security guards approach them, order Toby to remove his cap and ask them all to move on. When Ben starts to protest that they have no right, he is informed curtly that if he would like to come to the manager's office they can give him a copy of the shopping centre's policy.[169] For once he takes his sister's advice not to argue, and they walk back to the car.

14.3. Whilst the children and Geeta are all in the car with the luggage and presents, the parents pick up milk, bread, salad, pizzas and a bottle of wine, and proceed to the check out. They would all eat together that evening, and then Yasmin would drop Geeta back to her flat. As he opens his wallet, Gareth realises that he hasn't got any British money to pay for the shopping – only a few US dollars that were left from his holiday. In any case they usually pay with their NSC credit cards because the more he uses it the more money off vouchers they gets sent, and the greater their credit limit. They like the money off vouchers because they all related to things they'd bought at NSC in the past and sometimes they use them to try products they wouldn't usually buy but at a cheaper price.[170] Gareth places the card in the reader, and enters his PIN. The green and black screen of the reader flashes, telling the checkout operator to seek further authorisation for the card. As he gazes at the screen in disbelief, Gareth feels his mobile vibrate in his jacket pocket. It is the NSC bank fraud team! A formal, female voice informs him that they are investigating an unusual pattern of activity on his card.[171] Is he aware that it had been used recently in Florida, and is now being used in London? 'Of course' he answers. As he was explaining to the bank about the holiday, Yasmin hurriedly produces their other joint

[168] He had fitted the car with a top of the range Snooper S4 Evolution Camera Detector, which according to its sales pitch uses the latest GPS technology. It will locate all types of fixed Speed Cameras such as Gatsos, Truvelo, SPECS, mobile, DS2, Watchman and SpeedCurb. It has voice alerts and will even tell you the Speed Limit at every fixed camera it locates. With over two million people prosecuted as a result of automatic speed cameras and red light enforcement in car camera sensors are becoming increasingly popular for those who have to drive as part of their work. Details of these and similar products can be found at: SpeedCameraDetectors.Com (2006) 'Snooper Speed Camera Detectors,' http://www.speedcamerasuk.com/snooper-camera-detector.htm .

[169] The security guards were alerted by the in-store CCTV system and are under strict instructions to enforce the centre's guest conduct code. This states (among other things) that it does not permit: 'Any intimidation of our Guests by groups or individuals. All groups of more than five without the intention to shop will be asked to leave the centre' or 'Unsociable behaviour that is detrimental to the centre environment' and the 'wearing of any item of clothing which restricts the view of one's head/face (e.g.: hoods or baseball caps) with the exception of religious headwear' see, e.g.: Bluewater Shopping Centre's *Guest Conduct Policy,* http://www.bluewater.co.uk/home/guest-services/facilities/guest-conduct .

[170] The origins of consumer data are discussed in the 'Key Developments' section of the Consumer Surveillance Expert Report.

[171] Consumer data fraud is discussed in the 'Critical commentary and future directions' section of the Consumer Surveillance Expert Report.

credit card to pay for the goods, as well as her Reward Card.[172] [173] But, entering her PIN, the card is refused. Apparently they have spent up to her credit limit in Florida – strange that they hadn't realised. By now Gareth has come off the phone, and is able to pay for the shopping on his newly re-authorised credit card. They return to the car just as Geeta had succeeded in placating three bickering, jet-lagged kids, and go home.

15. At home

15.1. At their house in Finchley, North London, Ben and Toby unload the luggage, and Yasmin opens the front door. Their neighbours, whom they had asked to collect their post for them, had apparently been away for a few days and Yasmin has to practically shoulder-charge their ageing UPVC door just so she can squeeze through the enormous pile of letters and papers on the other side. 'What makes us so popular all of a sudden?' she thinks. With the family clamouring to get in, she gathers up the mail and dumps it all on the kitchen table. After unpacking and with a nice cup of tea in hand, Yasmin starts to sort through the letters. She pulls out the usual credit card bills, bank statements, council-tax notices and local free papers. She also finds two letters for Ben, and three addressed to her and Gareth which look like they are from Toby and Sara's respective schools. The rest are unaddressed items,[174] insurance and double-glazing offers, cosmetic samples, sportswear catalogues and even one, which catches her eye, about cheap flights. 'A bit late', and she has to laugh as she finds another about pet products addressed to their pet Labrador, 'Dan Jones'. They have recently taken out pet insurance for him and obviously forgot to tick the mailing list 'opt out' box.

15.2. She opens the three school letters. The first is a letter from Sara's school inviting them to a parents meeting to discuss the proposal to introduce random drug testing for pupils. As the letter explains, during recent trials in Kent, one school has seen its exam scores increase dramatically, and out of 600 tests carried out on the 11–18 year olds only one tested positive, which suggests the scheme was having the desired effect. As this was a controversial move the school wants to consult as widely as possible before making a decision.[175] The second letter, also from Sara's school, details the new access card-based systems that will be implemented during the first week of the new term. The system will also be used to monitor attendance and, the letter went on, in view of Sara's poor record last year, they will be using the system to provide parents with a monthly statement of attendance.[176] If there are any unauthorised absences they will be invited to the school to discuss the matter. Yasmin's heart sinks as she realises that they will have to have words with Sara about this. But her mood lightens reading the letter from Toby's primary school: it appears that she will now be able to see exactly what Toby eats for lunch each day. The school is installing a cashless payment card to pay for school dinners. As part of this scheme, parents will be able to access their child's purchasing record over the

[172] Consumer loyalty schemes, are discussed in the 'Critical commentary and future directions' section of the Consumer Surveillance Expert Report.

[173] The Reward Card enables her to collect points at a number of outlets, including NSC supermarkets, Johnson Holidays, and Wilsons, a national chain of travel agents. In fact, by booking the holiday with Johnson Holidays, she has collected enough Reward Points to afford a city break she has seen advertised in the window of Wilsons. She wants to surprise Gareth on their wedding anniversary later in the year. In popular loyalty schemes, such as the Nectar card, loyalty points are awarded for every £1 spent in participating retail outlets. For example, one Nectar point is worth 0.005p at Sainburys or Argos, and can also be redeemed in a number of other outlets. For details, see: http://www.consumerdeals.co.uk/nectar.html .

[174] Royal Mail's 'Door to door' service enables advertisers to get blanket coverage by postal code rather than individual addresses, http://www.springglobalmail.com/royalmail/en/d2d/d2d.htm .

[175] Blair, A, (2006) 'Teenagers to face random drug testing at all schools,' *Times Online*, 31 May, http://www.timesonline.co.uk/article/0,,2-2204492,00.html .

[176]. The system will also allow for 'full trial reports of pupil, staff and visitor movement' and enable 'system users to see who has entered what areas and when,' g2is (nd.) 'Access Controls Solutions for Schools' http://www.g2is.co.uk/pdfs/G235-G2_Access_Solutions_Schools.pdf .

Internet. Yasmin has always suspected that Toby buys crisps rather than fruit with his lunch money; now she will be able to check![177]

15.3. Ben skulks off to his bedroom to open his letters. The first informs him that his Criminal Records check is clear and that he has a place on a VSO[178] scheme to spend six months working with deprived children in Africa on a sustainable development project.[179] He is overjoyed, but the second letter brings him down to earth a bit. It asks him if he wants to take part in the UK national junior badminton team selection competition. Ben will have to think about this. He has played for his school at county level but he knows that if he plays in any national competition he is more likely to be have to take to a random drug test. Over the past few months he has been smoking a bit of weed at weekends, and he is worried that this might show up on the test.[180]

15.4. After dinner Yasmin drives Geeta the short journey to her flat. When Geeta's husband, Deepak, had passed away, Geeta would have preferred to have moved in with her daughter's family but there just wasn't the space. Instead the family had managed to get a sheltered flat for Geeta nearby. It is getting dark as they pull into the car park but Yasmin barely notices as the flood-lighting in the car park makes it feel like day anyway. Nor does she notice the CCTV cameras covering the entrance to the block. These enable Terry, the concierge, to keep an eye on the comings and goings, from the comfort of his office. As Geeta's electronic key fob opens the automatic door into the lobby area, Terry is already there to greet them and help with their baggage.[181]

15.5. While Geeta starts to unpack her things, Yasmin checks on everything in the flat. She turns on the water, electricity and gas and the movement sensor in the corner. Since Geeta had slipped and knocked herself out a few months ago, the family had asked for a movement sensor to be installed for their peace of mind.[182] Once Geeta has settled, Yasmin returns for an early night as she has to go straight back to work the next day.

16. In the city

16.1. Toby doesn't start back at school for another day and Gareth has taken an extra day off. It is a day full of chores; the car needs washing, they have to buy Toby some new school shoes and a mobile phone, and they have also planned to visit his mother, take her for lunch and shopping. Gareth's mother lives on the other side of

[177] 'Control of children's eating behaviour outside of the home is becoming an important issue' and via the Web, 'g2 cashless solutions offer parents the ability to load value to the child's card, monitor and manage daily spend allowances, view and even restrict purchases of specific food types bought,' g2is (nd.) 'Cashless Solutions for Schools' http://www.g2is.co.uk/pdfs/G231G2_Cashless_Solutions_Schools.pdf

[178] Voluntary Service Overseas.

[179] Criminal Records Checks are now mandatory for persons seeking employment in jobs involved with the care of the young or vulnerable. See Crime and Justice Expert Report

[180] As part of the UK Sports 'National Anti-doping Policy' all national sports associations must implement random drugs testing procedures. Testing potentially applies to all participants, taking part in any competition organised or affiliated to the national associations. In 2005/6 some 7,968 tests were conducted across 50 sports, of these 161 related to badminton, UK Sport (2006) 'Drug free sport', http://www.uksport.gov.uk/pages/drug_free_sport/ .

[181] Terry is employed by a private security company, and his job is to watch the CCTV monitors, listen on his audio system to any conversations and events in the block's public areas, and keep an eye on people coming and going from the block. If he hasn't seen someone arrive or leave for two days, he is instructed to check on individuals and report anything suspicious or of concern to the police, health or social services. See: McGrail, B. (1999) *Highly Thought of? New Electronic Technologies and the Tower Block*, ESRC Virtual Society? Programme Research Report, Milton Keynes: The Open University.

[182] In summer 2006, Cheshire County Council unveiled a 'telecare scheme', which funds the installation of monitoring equipment in the homes of the elderly to help them retain their independence. Stairlifts, rails, panic buttons, sink and bath flood detectors and movement sensors, which detect whether a person has got out of bed or fallen over are all part of the package. The movement sensor can detect the form of a body within an accuracy range of 12 pixels, see: Cheshire CC (2006) 'Alarms for elderly and disabled', http://www.cheshire.gov.uk/socialcareandhealth/adults/alarms_for_elderly_and_disabled.htm .

London, and Gareth reluctantly decides it will be quicker to drive through the centre of the city.

16.2. This means going through the Congestion Charging Zone, and Gareth asks Toby to remind him to log on to the Transport for London website when they get home so he can pay the congestion charge with his credit card.[183] Their number plate, 'GGJ 456' is read by the ANPR system, however some mud on the registration plate means a '5' is recognized as a '6' and their details are read entered incorrectly into the database[184]. Leaving the CCZ, Gareth turns into a service station to get the car its much needed wash. On the way out of the garage, at the entry to the one-way system, Gareth is unaware that another, police-operated, ANPR camera has read his number plate – this time correctly. Had he known, he would have been concerned to note that his vehicle was positively flagged to a mobile team of intercept officers positioned a few hundred yards down the road. This is because he has a criminal record for drinking and driving. But, as the conviction is over 4 years old years old, it is 11 o'clock in the morning, and the car is being driven in an acceptable manner, the team decide not to stop the vehicle[185].

16.3. While his mother does her shopping, Gareth and Toby go to 'Mobiles4You' to buy a new phone. Toby has been on about getting a phone for ages, most of his school friends have already got one, and he thinks it would be decidedly cool if he turns up at school with a brand new phone with loads of good games. Actually, Gareth is pleased that Toby is so anxious for a phone because, now that he is travelling to and from school by himself, Yasmin wants to be able to keep in contact. What they haven't told Toby was that they also plan to register the phone with 'Trace a Mobile.com' which will enable them to keep track of their son's whereabouts without him knowing.[186]

17. Crime and Society

17.1. Yasmin is relieved that on her first day back at work she has managed deal with all her emails and the urgent post by lunchtime and can use the afternoon to prepare for the Youth Inclusion Project (YIP) meeting later in the week. There is only one really urgent matter to deal with: one of her clients, Wilson Green, has broken the conditions of his curfew. Some months earlier Wilson had been designated as a Persistent and Prolific Offender by her Youth Offending Team and, as a result of some good intelligence and a police surveillance operation, had been caught red-handed breaking into a local chemist's shop[187]. He could have received a custodial sentence but was offered the chance to be enrolled on the Intensive Surveillance and

[183] The Congestion charge system utilises an automatic licence plate recognition system, which logs the number plates of all cars that enter and exit the charging zone on a data base and all cars that exit it according to the Transport for London (TfL) web site: 'After the vehicle registration number is read, it is compared with the database of vehicles which have paid their congestion charge for that day. … Following a final check at midnight (the following charging day), the computer will keep the registration numbers of vehicles that should have paid the charge but have not done so (including charges paid for the previous charging day). We will then manually check each recorded image before issuing a penalty charge notice.' TfL (nd.) 'Congestion Charging: imaging and cameras,' http://www.cclondon.com/imagingandcameras.shtml .

[184] The implications of this for Gareth are negligible: technically he has not been registered on the system so he wouldn't have to pay the charge, but as he doesn't know this so he will pay the charge anyway. The consequence for the driver of the car GGJ 466, who is currently driving her vehicle on a touring holiday of France, will depend on whether the manual check carried out before a penalty notice is issued picks up on the fact that they are different vehicles – in fact they look very similar.

[185] This camera is operating as part of the national roll out of the ACPO ANPR Strategy. See Crime and Justice Expert Report.

[186] 'Location Services are designed to locate the phone of another person. For the service to work, the phone has to be switched on and within network coverage. Location services aimed at children are intended to complement, not be a substitute for, normal parental supervision. They give information about the location of a child's phone and, in conjunction with other types of communication, such as phoning or testing, can help parents keep in touch with their children,' Trace a Mobile.com (2006) 'Mobile phone tracking guide,' http://www.traceamobile.co.uk/mobiletrackingguide.php .

[187] Dunnighan, C. and Norris, C. (1999) 'The detective, the snout, and the Audit Commission: the real costs in using informants', *The Howard Journal*, 38(1): 67-86

Supervision Programme instead.[188] However, they have now been informed by Track-and-Trace, the private company responsible for running the electronic monitoring scheme, that in the last two weeks he has broken his curfew three times. As a result Yasmin will have to attend a case conference called for the next morning to consider whether they have to send him back to court and face the possibility of prison. 'How depressing' she thinks.

17.2. But being assigned to the YIP is more positive. Whereas most social work is about picking up the pieces after things have gone wrong, the YIP programme tries to identify those young people most at risk of becoming offenders, and provide them with positive support before they get into trouble. On Friday they will be having a multi-agency review meeting to determine the final list of those who will be included in the programme. The programme is focused on the place Yasmin thinks is the worst housing estate in the borough: the Dobcroft Estate. This is a sprawling 1960's high-rise estate with over 2000 flats and a maze of concrete walkways. She knows that most of the kids on the estate would benefit from the support they could provide, but they have to be selective in targeting only those most at risk of future offending. The interventions include: getting them involved in local sports activities; attendance at drug-education and anger management classes; getting their mums and dads to attend parenting classes; and – the one she liked best – getting them to make short films about the problems faced by young people in the area. She is always surprised by how much they seem to gain from the experience.[189]

17.3. Before Yasmin had gone on holiday she had asked all the local agencies involved with children to fill in a risk-assessment form 'for all the young people aged 13-17, resident on the Dobcroft estate, whom you are aware of as being at risk of offending through your work with them or their family'. She had already received replies from the local schools, the police, social services, Connexions, the Local Education Authority, and the Youth Justice Board. In order to ensure that no one slipa through the net, she had also contacted the local tenants' association, the outreach drug team and the Neighbourhood Watch coordinator to ask them to nominate any children who had come to their attention. Each agency was asked to rate the child's risk of offending on a scale of 1-5, and provide key information which would be used to determine the overall risk score.[190]

17.4. She now has the task of collating all this information so that they can target the intervention at those most at risk. She decides that the easiest way to start is to sort the reports by name – and see if any child has been referred by more than one agency. There were many multiple referrals, but one name stands out: 13 year-old Darren White. He has been identified by six agencies, he has been in local authority care but is now back living with his single-mother, his elder brother has a string of convictions even though he is only 17, he is a regular truant and is hanging out with

[188] The ISSP can insist on routine drug testing to ensure offenders are not engaging in substance misuse and subject offenders to a variety of additional surveillance measures. At least two checks have to be made each day, with the potential of increasing the surveillance to continuous 24-hour monitoring. The checks include: face-to-face monitoring by a probation office at specified times during the week and to accompany them to scheduled activities and appointments; electronic monitoring to ensure that curfew conditions are met; voice-print verification over the telephone to ensure that the person is where they say they are; and overt police surveillance 'of the movements of these young offenders at key times to reinforce the programme, as well as share information with the ISSP staff in the youth offending team, 'Youth Justice Board (nd.) 'ISSP: Surveillance' http://www.youth-justice-board.gov.uk/YouthJusticeBoard/Sentencing/IntensiveSupervisionAndSurveillanceProgramme/Surveillance.htm .

[189] See 'Key Developments' section of the Public Services Expert Report.

[190] The police form, for instance asks if the child has been arrested, convicted or had other contact with the police in the last six months; the school form asked if child the had been excluded from school over the last 12 months and whether they were truanting regularly. The form for the neighbourhood watch coordinator to fill in, asks whether the child has been causing a nuisance in the area, was involved in a negative peer-group, whether they were known to have been offending and whether their siblings or other family members had been involved in offending, Youth Justice Board Youth Inclusion Programme (nd.) 'YIP Core Group Referrals – Guidance For Partners' http://www.youth-justice-board.gov.uk/NR/rdonlyres/0233E9E7-8E58-45E0-ACF8-E3190B8EAD19/0/ID50guidancedocumentforpartners.doc .

a bad crowd, and is involved with drugs. And every referral has graded him as being a '4' or a '5' indicating a high risk of future offending.

17.5. By the end of the day she has identified 73 children who, on her preliminary assessment, will need to be discussed at Friday's multi-agency meeting. Tomorrow she will repeat the process for the Junior Youth Inclusion Programme aimed at identifying even younger children at risk: the 8-13 year old group.

17.6. On the way home, scanning a newspaper on the bus, her eye is caught by the headline '"We can clamp down on antisocial children before birth", says Blair'. As she reads the article, she wonders if the Prime Minister's plan to intervene with 'problem families' before their children were born to stop their children growing up bad, were going too far. But then again, she reflects, maybe it is just the logical extension of what she is doing already, another use of data to predict and control behaviour.[191]

18. The Call Centre

18.1. On Tuesday morning Gareth returns to work. He works as a client manager at the Sentasi Group, which owns several multi-client call centres.[192] As he swipes into the building using his RFID-implanted card, the time and attendance system simultaneously logs his hours. His photograph appears on a screen in the security office, where staff can locate his whereabouts as he uses the card to enter or exit different parts of the building.[193] His job involves managing two large projects. One involves his team cold-calling households to try and get them to switch their telephone accounts to his client, Novacom. The other is for an insurance company, which is targeting a 'niche product' called 'Platinum' aimed at older, safer drivers.[194] Customers also dial in to change their details, make claims, and cancel their policies.[195] He has to report performance results to his clients on a daily basis, and every week has to submit a written report to explain any fluctuations in the call statistics. His job has its perks. Apart from getting a monthly bonus based on the performance of the projects, he recently had the opportunity to work more closely with Novacom in setting up a dedicated call centre in Hyderabad. Getting to know his opposite numbers in the client company makes the job of reporting the statistics much easier.[196]

18.2. In order to get up to speed after his holiday, Gareth has arranged early meetings with the team leaders from both projects. The Novacom project is running well. He monitors how long each operator spent on each call and how many of their calls result in sales, and the monthly report he receives shows that even though he had been on holiday, performance hadn't dropped. Apart from the new recruits, who are still learning the job, most of his team are exceeding their sales targets. Gareth attributes this to good supervision and job design, and wonders whether he should

[191] Woolf, M., ''Failures' targeted at birth', *The Independent*, 16 July 2006, http://news.independent.co.uk/uk/politics/article1180225.ece .
[192] A 'multiclient' call centre is one whose core business is to provide contact services to different companies at the same time.
[193] See: 'Critical commentary' section of the Workplace Surveillance Expert Report.
[194] See: 'Key Developments', Consumer Surveillance Expert Report.
[195] Callers are placed in queues which have different wait times, and are routed to employees with varying skill levels. 'Gold' is answered the fastest and by the most skilled agents including team leaders. These customers have been insured with Platinum for over five years, and have fully comprehensive cover. 'Silver' has been insured fully comprehensive from 0 -5 years, and 'Bronze' handles all callers who have purchased third party insurance.
[196] In this situation, the client sees Gareth as being responsible for the performance of the project and so it is he who is under surveillance. As the person who delivers performance reports to the client (by email) Gareth is answerable for the statistics. Developing a more personal relationship with the client will help humanise this distant, technologically mediated situation.

increase the performance targets[197]. He will also recommend the team leader for a bonus this month.

18.3. Having been elated by the news from Novacom, the news from Platinum brings Gareth back down to earth. Because there had been a recent lull in calls, some employees have been surfing the Internet to pass the time. The company allows some private surfing, so long as the employees log out of the telephone system when they do so. This is because the telephone system records their activities every minute of the day. Every week, the computer summarises the project's performance using the statistics generated from the computerised telephone system. It is these statistics that Gareth has to communicate to the client.[198] Long periods of inactivity are not good news as far as the client is concerned. The IT department also stringently polices the sites that employees visited.[199] IT has reported that one member of staff is spending time on a private blogging site during working hours. Rather than block the site, IT has read the employee's posts and informed a team leader of their content in Gareth's absence. After the meeting, Gareth settles down to work through his outstanding emails and refresh his knowledge of the company's disciplinary guidelines.

19. Health

19.1. On Wednesday morning, Geeta is fed up as she is not allowed to have breakfast; not even have a slice of toast or a cup of coffee. Her calendar on the kitchen door reminds her in thick red pen, that today at 4.30 pm is her 'Well Woman Check'. Last month she'd received a letter from her GP asking her to attend the local 'Well Woman Clinic', aimed at patients over 50. The letter, written in English and translated into Urdu, explained how she, as an older woman, was at risk of heart disease,[200] stroke, diabetes, kidney and liver malfunction, and cervical and breast cancer. It emphasised how early diagnosis of any of these diseases increased survival rates, and that her health and well-being were important. Reading it made Geeta feel like her life was on the line, and she wondered why some of these tests were necessary.[201] The letter advised her not to eat or drink anything, except water, in the 12 hours preceding her check, as they would be taking blood and urine samples. They would also be checking her height, weight and eyesight. The letter also explained that the nurse would talk to Geeta about her lifestyle and diet, and could make recommendations. It also said something about attending hospital for breast screening if necessary.

19.2. Geeta feels daunted as she remembers how she had looked after her own parents with very little medical help. But she is pleased that the NHS knows so much about her and is looking after her so well.[202] Both her parents had died of heart attacks, and it still worries her that she might have the same problems. She hasn't had much

[197] In doing this he also allows experienced team members to develop their own sales pitch although he makes a point of listening to a random selection of calls to ensure they are not straying from company guidelines. See: 'Key Developments', Workplace Surveillance Expert Report.
[198] In call centres, employees work at a desktop PC, attached to which is a small console called a 'turret'. The turret has a number of buttons that employees must press, which relate to each aspect of the job. The buttons relate to different 'Activity Codes' e.g.: 'Not ready for a call' (Not Ready); 'ready for a call' (Ready); 'taking a call' (Call); 'wrap up from a call' (Wrap); 'Auxiliary codes' (Aux Works) – the latter pertain to activities such as filing, answering emails, and breaks. The client and the call centre management will agree time limits for each activity code and staff times are monitored closely and scored. The scores are averaged out over time and used in appraisal and performance review.
[199] See: 'Introduction', Workplace Surveillance Expert Report.
[200] British Asians (with origins in Pakistan, India, Bangladesh or Sri Lanka) are at higher risk of coronary heart disease see *Patient UK* (nd.) 'Preventing Cardiovascular Disease,' http://www.patient.co.uk/showdoc/23068754/
[201] See: 'Key Developments', Medical Surveillance Expert Report.
[202] See: 'Key Developments', Public Services Expert Report.

contact with the British health system, having had both of her children at home in Pakistan, and having enjoyed good health for most of her life.

19.3. She had asked Yasmin to come with her, but she can't because of work commitments. However Sara had offered to accompany her, as she could just make it after school. Geeta is really pleased that her teenage granddaughter would make the time. While they are on the bus, Geeta keeps quiet about her worries, and Sara distracts her with a rant on the workings of CCTV, prompted by the sign on the bus saying that 'in the interests of safety and security of their passengers this bus is equipped with CCTV monitoring' and her recent experience of having been barred from their local shopping centre because she had the audacity to question whether the security guards had the right to make her and her mates leave "just for sitting on a bench". Geeta thinks there might be more to this story but agrees with a conspiratorial smile, and much to Sara's relief, not to tell Yasmin.[203]

20. School and after…

20.1. On Wednesday at Ben's school the corridors are packed with lost students looking for classrooms. For once, he has left himself enough time to find where he has to go. His class isn't until midday, so he heads for the cafeteria to see if he can see anybody he knows. But there isn't yet and he as there is a computer free in the Internet café he grabs the place, mostly so he can people-watch from a safe distance. He doesn't need a school log-in to get onto 'Net, so it is the perfect opportunity to check his hotmail account before class. His inbox contains 120 messages, hardly any of them from names he recognises. Apparently, various provocatively-named females want to show him a good time, he can get 'herbal v1agra' (sic) and other dubious drugs for conditions he can never imagine having, he can even have cheap breast enhancement or make millions if he just helps out the ex-wife of some Nigerian ex-cabinet minister. He paused for a second, and then deleted them all. Another email is supposedly from his bank asking him to confirm his online log-in details. Ben is not that gullible and knows all about these kind of scams, so he deletes that too. He does wonder why he keeps getting all this junk e-mail though.[204]

20.2. Finally, he notices something from his friend Aaron, with whom he'd done his A-levels the year before. Like Ben, Aaron is involved in anti-capitalist activism. They have been on Critical Mass and Stop the War events together since they were 16, although Ben's parents don't know about this. The message says that there will be an anti-capitalist demonstration in London the following Saturday, that it is being organised in secret, and that he has to text a mobile phone number to get the details of where to meet. Ben replies straight away saying that he will see Aaron at the local tube station on Saturday morning. He is hoping he can get some money together between now and then. That afternoon he has to go to the benefits office to see if he can claim Jobseekers Allowance, and is even considering his father's offer of a part-time job in the call-centre albeit reluctantly.

20.3. The news from the Benefits office is okay, but Ben was annoyed because they won't give him a clear answer. They have told him that because he is studying one A-level part-time, he can claim Jobseekers Allowance, in theory. However, before they can make a decision he has to fill in a questionnaire to give to the adjudication officer, who will decide, over an unspecified period of time, whether or not Ben

[203] On exclusion policies of shopping malls, see: McCahill, M. (2002) *The Surveillance Web*, Cullompton, Devon: Willan.
[204] See: 'Critical commentary and future directions', Consumer Surveillance Expert Report; Wall, D (2001) Mapping out cybercrimes in a cyberspatial surveillant assemblage,'. In Ball and Webster (2003) *op cit.* n.149.

really is a 'job seeker'[205]. He reckons that his mum might know what the situation is, but he suspects that she would just say that it would take ages. She often comes in from work complaining about how impossible it was to get the right information from people working in other areas of social services.[206]

20.4. In the meantime, Ben needs to find some money for the weekend, so he goes back home and calls his bank for a balance and, if need be, arrange a small overdraft. Ben is pleased that he decided to use his parents' phone to call his bank, rather than his pay-as-you-go mobile, because they keep him on 'hold' for ten minutes. Then he has to answer four security questions: date of birth, mobile number, occupation, and postcode before they will tell him anything. Luckily, he has just enough money. After reading the jobs sections of the local free papers that had come through the door whilst they were away, he heads back to school to check out the sports centre.

21. Family

21.1. Early Thursday morning, as Gareth contemplates what looks like being a very difficult meeting, he feels guilty. Even though he has almost recovered from his jet lag, he had left home in a bad mood. He is frustrated with Ben, and suspects that he has been mixing with 'the wrong crowd', as he does with Sara, and maybe even taking drugs. Ben has been acting strangely – he seems more lethargic than usual – and Gareth is worried not only for his son's future but also for the example he is setting his little brother. That morning, he'd shouted at Ben as he refused to get out of bed, before snapping at Yasmin who was already lecturing Sara about being ready for school in time. Neither of them want to see another terrible attendance report, now generated by the indisputable evidence from her RFID-implanted tag.

22. The Call Centre again

22.1. His thoughts soon turn to his meeting with the employee suspected of abusing company computing facilities, and the HR and IT managers. Since the briefing with the team leaders on Tuesday he has received some documents from IT detailing the employee's Internet activities. He is wondering how he will deal with it. The employee, Asabe, has been writing a cynical blog about working in a call centre. Most of the blog has been written in her own time from her home computer, but when he compares the information provided by IT with the staff roster, he spots that she has also been posting in work time.[207] On the other hand, when he double-checks Asabe's performance statistics for the last couple of months, he sees that she appears to be a top performer. She has been taking the right number of calls, achieving incentives set for quality, resolving most queries first time, and her timekeeping is excellent. She has kept to her allotted times for lunch, tea and bathroom breaks. On paper there isn't a problem.[208] Gareth is relieved.

22.2. In the meeting, Asabe, who was originally from Nigeria, explains herself. The blog contains anonymised stories about her encounters with managers and colleagues in the call centre. It turns out that Asabe has been feeling victimised by jealous colleagues because of her high performance, and feels she has been bullied. Sadly, her skin colour has become the focus of the bullying. She feels that her team leaders have turned a blind eye to it even though she has informed them of her concerns. Because she needs the work as she is saving up for university, instead she

[205] The Advice Centre (nd.) Funding and benefits: Part-time students,' http://www.advice-centre.info/Part-Time%20Benefits.pdf#search=%22benefits%20for%20part%20time%20students%22
[206] See 'Key developments,' Public Services Expert Report.
[207] See: 'Critical commentary and future directions', Workplace Surveillance Expert Report.
[208] See: 'Key Developments', *ibid*.

has taken to blogging about her experiences to deal with the stress. Unfortunately Asabe has unintentionally revealed the location of her workplace in the blog. In the meeting the legal problems were aired: the company has been publicly identified and its management criticised in a manner that could lead to legal liability under the Race Relations Act if Asabe decides to take them to an employment tribunal. One of its top performers was in danger of leaving. What was more, Asabe is now outraged because she has been snooped on by her employer. A tense stalemate ensues.[209]

22.3. As the meeting ends, HR had resolves to investigate the allegations of bullying. They encourage Asabe to keep a less public record of the incidences where she felt bullied, and to keep her team leader informed so they can identify the culprits. However Asabe now feels doubly aggrieved: she has been the target of bullying *and* surveillance. She says she will be looking for other work and will consider taking legal advice. Gareth wishes he had been around to help the team leader deal with the initial situation. His instinct is that the whole matter should have been dealt with more quietly, and that the company should have supported Asabe, rather than pursuing its own legal interests.[210] Looking forward to the weekend, he hopes that the rest of the week would be quieter.

23. Fraud

23.1. Friday is a mercifully quiet day. As everyone returns to Finchley in the early evening, a relaxing weekend is in store. Then as Gareth and Yasmin are preparing dinner, she brings up the subject of their joint credit card bill which has arrived whilst they were at work. They both know they have spent a fait bit on holiday, but it has slipped Yasmin's mind that the card had been refused earlier in the week, so they both gasp at the size of the bill. Not only that, the card had maxed out on transactions that they do not recognise at all: purchases at clothing stores and restaurants in California appeared on the bill, but they did not even visit California. More worryingly, is seems that that the card has been used to pay for access to websites with names that sound pornographic and perhaps worse. Yasmin is horrified. She has recently read about a pop star who has been put on the Sex Offenders Register for accessing such child pornography sites. If she is investigated what will her bosses think? Even if she is innocent, which of course she is, tongues will wag and rumours will spread. She could even lose her job. Momentarily she is tempted to check what these websites are all about on her home PC, but she realises that this will only lead to evidence of her having visited the sites being recorded somewhere in the depths of her computer.

23.2. Instead, Gareth immediately calls the customer services number on the bill. He punches in their account details, and is transferred to an operator with a South African accent, within seconds. He explains the situation. The operator cancels the card straight away and said that in their case the credit card company would refund the money lost to the account. They also advise that Gareth should inform the major the credit-rating companies and inform them of the situation. He goes online and applies for a copy of his credit record, and asks for regular email updates to see whether any fraudulent credit applications have been made in his name.[211]

23.3. Feeling thoroughly harassed, Yasmin, Gareth and the kids eat dinner together. Soon, Sara disappeara upstairs to listen to her favourite music; Toby goes to play games online on the PC and Ben mutters something about 'getting his stuff together

[209] See: 'Regulatory issues', *ibid.*
[210] See: 'Key developments', *ibid.*
[211] Inside Out –East (2003) 'Credit Card Cloning' *BBC Online*, 7 July, http://www.bbc.co.uk/insideout/east/series3/credit_card_cloning.shtml

for tomorrow'. Yasmin and Gareth retire to the sofa where they gaze vacantly at the news and eventually fall asleep.

24. Back in the city

24.1. On Saturday morning, Yasmin and Toby go for their weekly swim. As they walk towards the tube station, Yasmin notices a Neighbourhood Watch sign, which reminds Yasmin that she needs to renew her registration. At the station they have to queue to buy Toby a ticket. This was annoying as Yasmin has an Oyster Card which she thinks is excellent as she doesn't have to worry about having the right change for the turnstiles anymore. She just passes the card over the 'reader' as she goes through the barriers, and the fare is automatically debited to the Oyster Card. Now that she has subscribed to automatic online top-up, her card never runs out of money, so long as there is money is her bank account.[212] As they wait on the platform Yasmin is aware that they are being monitored by the London Underground's extensive network of CCTV cameras[213]. One in the swimming pool, however, although she is knows that they are watched over by lifeguards, she does not realise that they are also being monitored by 'Poseidon: the lifeguard's third eye' which automatically detects any incidents of potential drowning[214].

24.2. Ben also uses his Oyster Card today as, according to the text message he had received from the 'Stop the War' organisers, he had to be at a Tube station that could receive mobile phone signals at 12 o'clock, and be wearing either a baseball cap or hooded top, so that his face would be less easy to capture on CCTV. Then, he would receive a text message telling him where to rendezvous with the other protestors, and saying that he would need to get there within 45 minutes. At the station, he easily spots his mate Aaron and the organisers, who tell them to walk in ones and twos to Grosvenor Square, and to converge from the surrounding streets on the American Embassy at 1.30 precisely. Then, a huge banner will be unfurled, proclaiming 'Stop the War', they will try to deliver a protest letter to the ambassador, and a spokesperson will read the contents of the letter, in front of the banner. This will all be filmed, and broadcast live on their web site. The whole event is due to last less than two minutes after which they will disperse and go their separate ways.[215] The protest goes off as just as planned. By the time the police have arrived Ben and Aaron, having retrieved the banner, are well away and were walking through St. James' Park on their way to Waterloo Station, to meet up with some of the other protesters and catch up on the protest news. En route they have to pass Parliament, and in an act of bravado, Aaron hurriedly unfurls the banner, drapes it over the big black railings, hands Ben his mobile phone, and asks him to take a picture. As Ben is zooming in, he feels a hand on his collar, and a voice says, 'You're under arrest!'

24.3. Three hours later they are released from police custody, with only an informal warning.[216] Although they were questioned, photographed, fingerprinted and DNA swabbed they are relieved that no further action was taken against them.[217]

---

[212] . The oyster card is a smart card that uses an RFID tag to identify the owner and keep a log of their journeys. This is necessary because if you 'make several journeys on the same day, once the total cost of these journeys reaches a cap, any further journeys you make that day will be free, unless you travel beyond the zone(s) covered by your original cap,' TfL (nd.) *Oyster On-line*, http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp .

[213] See: McCahill and Norris (2003) *op cit.* n.44.

[214] 'Poseidon' uses computer vision software to identify possible drowning incidents, for instance a body that remains still underwater for ten seconds or more, Poseidon (nd.) 'Technology overview', http://www.poseidon-tech.com/us/technology.html .

[215] These are all counter surveillance measures. They know the police monitor their web site, and suspect that their phones are tapped. By only revealing information at the last minute and using a newly purchased mobile phone to send the text messages they believe this will lessen their chances of interception.

[216] Technically they have breached the new law banning protest within one kilometre of the Houses of Parliament without prior police approval. See: 'Parliament protesters fight ban' *BBC News*, 31 August 2006, http://news.bbc.co.uk/1/hi/england/london/5303558.stm

24.4. Unknown to the boys an intelligence report was filed by the arresting officer, which, an hour later, was scanned by an officer investigating the earlier 'spontaneous' protest outside the embassy. He is intrigued that they had travelled to Marble Arch station, and suspected that this was the meeting point for the protesters. He wonders if he could request permission to access the Oyster Card database and gather all the names of people who finished their journey at Marble Arch earlier today.[218] It would be great if he could identify all the protestors, but then again they would probably be far too many to sift through and he is unsure if he would be granted permission under data protection laws for such a blanket disclosure.[219]

24.5. It is late when Ben finally arrives home that night. He has been for a few drinks with Aaron, and creeps in after everyone else has gone to bed. Even Sara, who has taken to hanging out with her friends in the local burger joint until it shuts at 11.30, is back. In the kitchen, he fills a pint glass with water and quietly climbs the stairs, gently shuts his bedroom door and turns out the lights.

25. Conclusion

25.1. Is this week in the life of the Jones family so out of the ordinary? A lot of the surveillance they encounter, much of it automated and out of sight, is met by most members of the UK public on an everyday basis.[220] Surveillance of international travel, of mobility in urban space, of consumer spending, of Internet and mobile telecommunication and of potential criminal activity is now an everyday occurrence. Some of this is of benefit to such a family, and is appreciated, but much of it is also personally threatening and has wider consequences. We have shown that surveillance intensifies in a number of different situations: where a person is vulnerable, whether they are about to transgress a legal or organisational rule, and even where they are relatively empowered. The eldest and youngest members of the family find that they are having their movement, whereabouts and the content or state of their bodies tracked 'for their own benefit and safety'. This is conducted through schemes and products which are currently widely available and publicised to the UK public and opted into voluntarily by the family members.

25.2. Surveillance is intensified when family members are either a suspected perpetrator or victim of a crime. Deviance takes on a new meaning in the private spaces of the workplace, shopping mall and school, where organisation-specific rules define what is and is not acceptable behaviour. Different intensities of surveillance occur which are aimed at either resolving 'difficult' situations or removing people altogether. Consumers can also break rules: surveillance of consumers privileges some but disadvantages others. This was illustrated in the case of credit cards, loyalty cards and junk mail which feed and flow from the consumer profiles of Yasmin and Gareth enabling them to purchase particular kinds of products at reduced prices, whereas Ben, being a low-status customer is forced to wait on hold to talk to his bank at his own cost. Patterns of unusual activity, however, highlight the ever-present gaze of the bank. In all cases, any unusual or unexpected activity in

[217] Police can now take fingerprints and DNA samples of all persons under arrest even though they have not been charged with an offence. These will remain on the national databases. See: Johnston, P (2003) 'Police to keep DNA files of innocent,' *Telegraph.co.uk*, 27 March, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/03/27/ndna27.xml .

[218] An example of function creep: after the Oyster Card system was introduced as an easy way of paying for public transport, the police realised that such data could be useful in criminal investigations.

[219] In 2004 the Met made only seven requests for Oyster card journey information, in 2005 this had increased to 243 requested which were granted on 229 occasions. See: Jones, S (2006) 'Oyster cards used to track criminals,' *The Guardian*, 14 March, http://www.guardian.co.uk/crime/article/0,,1730518,00.html .

[220] Both Yasmin and Gareth hold jobs which involve comparatively large amounts of surveillance, which allows us a more focused discussion.

relation to one's category in a database, intensifies surveillance, with varying consequences.

25.3. What is significant about this set of events? Apart from the fact that they reflect much of our everyday experience, they highlight many of the issues with which this report is concerned: in particular, the antecedents, consequences and experiences of surveillance. The family encounter a wide range of surveillance, some of it overt and explicit, some it covert and in the background: a full list of all the surveillance encounters is provided in the appendices. In some instances, they make a choice to engage with surveillance, at others they do not. When outside the family home as citizens, consumers, travellers, and workers the family exercise little choice as to whether they are subject to surveillance. In the case of consumer products, the airport, and urban surveillance by police and CCTV, the family are unaware of the extent of information held on them, and surveillance occurs as a normal element of infrastructure. In the case of health screening and surveillance in schools, recipients are advised to submit to it 'for their own good', which raises questions about the kinds of choices being made. Any meaningful debate about the surveillance society will rest upon the public having at least some knowledge of what information is held on them, where it goes, what is done with it and why. It will also rest on what can be done to regulate the excesses of surveillance, and by whom.

25.4. In spite of this variation, the surveillance processes we have highlighted have one thing in common: they all affect the family's life chances, decision-making and relationships. Privileged consumers, such as Gareth, access services faster than his impoverished student son, Ben. Vulnerable people, such as Geeta and Toby, have the boundaries of their homes and bodies monitored, and lose autonomy and privacy in the process. Even being considered as merely suspicious changes behaviour. Yasmin is conscious of her criminal records check, and Sara dares not answer back to security guards. The prospect of being excluded, or having the terms of one's engagement with society change, emerges as a stark consequence, and appeals to the family's deepest anxieties. Hence, it is not surprising that the family shows a great deal of ambivalence towards it. Yasmin and Gareth, at various points, use surveillance techniques in an empowering way to protect their own credit ratings, monitor their children's and Yasmin's mother's health and well being. At work they use their own social networks and relationships to mediate and interpret surveillance data. In particular, the introduction of surveillance into the childrens' schools highlight family relationships, and exacerbates existing tensions. The range of experiences of surveillance exercised upon and by the family, mean that addressing 'surveillance society' as a single and monolithic phenomenon is unwise. It is dynamic, multilayered and complex. The question now concerns what will happen next.

Part C/2: Glimpses of Life in the Surveillance Society, 2016

26. Introduction

26.1. Danish physicist, Niels Bohr famously quipped that "Prediction is very difficult, especially if it's about the future." We did not want to get into the business of futurology or prediction here, however we thought it would be useful to provide a few vignettes which take some incidents from the scenario and throw them forward a short time into the future, to indicate some of the changes which regulators will have to anticipate. We use the same cast of characters as for the 2006 scenario at the same stages of life and social position.

26.2. If we are to suggest overall themes they are that the future surveillance society will be one of pervasive surveillance, primarily directed at tracking and controlling mobilities of all kinds (people, objects and data) and at predicting and pre-empting behaviour. We also assume that the shift of power from public to private continues.

26.3. These glimpses should not be taken to mean that in practice all of the systems and processes here would all 'work'; as detailed in Section 9.11 above, technology has limits and plans fail. However for the purposes of the glimpses here, we have assumed that things work as advertised.

26.4. But these glimpses are also fairly conservative. This future is nowhere near as dystopian and authoritarian as it could be: we have assumed the same kind of mixture of care and control as has generally existed in Britain since WW2. They do not factor in the possibility of radical new developments – for instance complete ecological disaster, or world or civil war that might turn risk categories from rough stand-ins into dividing lines of violent conflict or conditions for genocide. That should not be taken as meaning that such things are not possible: they have happened before, are happening now in other parts of the word, and can happen again anywhere.

26.5. We present 14 vignettes, entitled:

- Identity Control
- Border Crossings
- Managing Brandscapes
- Cashless Shopping
- Keeping Tabs on Kids
- Total Social Solutions?
- Driving Change
- Friendly Flying Eyes in the Sky
- The Unidentified Underclass
- Virtual Tracking
- Your Life is Our Business
- Looking After You
- The Hall of Mirrors

27. Identity Control

27.1. Arriving back in Britain from Florida in 2016, the Jones family face a rather different scene than the family of 2006. It is hard to know the difference between the two countries by what they experience at the border. Both Britain and the USA's immigration and border control services, along with those of all EU countries, and other G10 industrialised countries are outsourced to the same transnational private consortium, BorderGuard.[221] Continued fears of illegal immigration and government rhetoric about the 'War on Terror' led these governments to commission and implement a 'smart border' scheme, driven by both open and hidden surveillance technologies.

27.2. Passport control is now a series of cameras ands scanners taking images of face, iris and fingers, which are compared to those on the standardised biometric passports, or in Britain's case, the ID card, introduced across the G10 countries and the EU.[222] The passport or ID card is also read by machine and the multiple data on the built-in RFID chip now include all citizenship, immigration, visa and criminal justice data, along with health information. This is instantly compared to state and transnational databases, as well as a whole raft of data-mined information on consumer transactions that BorderGuard gets on regular subscription from specialist companies.[223]

28. Border Crossings

28.1. The result of smart borders is that transit happens more swiftly for some, and less so for others, depending on whether their nation of origin has signed up to the scheme. BorderGuard has made concessions, however. It has allowed citizens from non participating countries faster transit if they have biometric passports. Pakistan, although not a member of the scheme, offers biometric passports to its citizens, but at a significant financial cost that individuals must bear personally.[224] Geeta has never bought a biometric passport and consequently has to wait for several hours and is subjected to various extra searches and questions.

28.2. Sara's deliberately shocking fashionable teenage appearance arouses no suspicion, but Yasmin's obviously 'Asian' features trigger alerts. When her ID card scan connects to her credit card records from the USA, she is pulled over for questioning.[225] She doesn't have to wait until she goes shopping to find out that what her cloned card has been used for. She is, however, required to explain away a

---

[221] See: Borders Expert Report

[222] The International Civil Aviation Authority agreed standards for Machine Readable Travel Documents (MRTDs) in 2004. This process has been driven by the current G8's Secure and Facilitated International Travel Initiative (SAFTI), see: *Statewatch* (2004) 'G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel', http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm . This is despite concerns over the ease of cloning of RFID chips: Johnson, B. (2006) 'Hackers crack new biometric passports', *The Guardian*, 7 August http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html . The fact that UK ID cards could easily morph into or merge with biometric passports has already been noted: Lettice, J. (2005) 'UK biometric ID card morphs into £30 'passport lite'', *The Register*, 8 July, http://www.theregister.co.uk/2005/07/08/id_card_as_passport/ .

[223] See Consumer Expert Report. In 2016 there are still ongoing issues between states and outsourced border security about the intellectual property issues around travel data. The UK government maintains its 'right' to sell ID data, as was proposed in 2006: Elliot, F., 'ID plans: powers set to widen', *The Independent*, 6 August 2006, http://news.independent.co.uk/uk/politics/article1216000.ece . The only voice that still remains lost is that of the citizen.

[224] There has been some consideration of these potential problems, see e.g.: Koslowski, R. (2004) 'International Cooperation to Create Smart Borders', Paper presented at *North American Integration: Migration, Trade, Security*, Ottowa, April 1-2. http://www.irpp.org/events/archive/apr04/koslowski.pdf

[225] Informal racial profiling undoubtedly already occurs and has occurred for a long time. It has also been suggested by UK police as a formal policy http://www.timesonline.co.uk/article/0,,22989-1717624,00.html For background, see: http://www.aclu.org/racialjustice/racialprofiling/index.html

whole range of dubious purchases in an area of the country that she hasn't visited. She is allowed to go an hour or two later after the data are cross-referenced with records in Florida and it is determined that her card has been cloned.[226] The bank will still not return the money to her account for several weeks – some things never change!

28.3. At customs, everyone is subject to a full-body scan: a virtual strip search using a millimetre wave scanner.[227] Sara thinks she hears one of the customs officers make a lewd remark about her piercings[228] but there's no point in complaining as it will just draw attention to herself and mean more trouble.[229] In any case, it's pretty likely that everything the officer said was recorded by the CCTV mics, which are used for work monitoring, and he may end up in trouble anyway.[230]

29. Managing Brandscapes

29.1. When the Jones family visit their local shopping centre, CCTV and security guards are still there and the centre managers still have their networks of contacts to spot the undesirables and keep them away from the shops and the shoppers. However, spatial modelling of the brandscape[231] and changing advertising according to the flow of different categories of consumer is now a strategic priority for most retailers; new business connections have developed between the owners of the shopping centre and its tenants, the large retail chains to this end.

29.2. The retail chains allowed the shopping centre access to a huge shared database, modelled on Reward Card data, to generate information about the flow of shoppers. The system relies on RFID clothing tags, ubiquitous scanners and consumer datasets. Scanners placed in the doors of participating shops log the unique identifiers found in RFID tags embedded in the clothes of shoppers. Information about the item of clothing, its brand, where it was purchased, and by whom, is compared against the consumer profiles of different wearers. Intelligent billboards placed at eye level display advertising from a select range of products aimed at that consumer profile in real time. Sara is delighted to see the new album cover of her favourite band appear on the screen to advertise the nearest music store and Toby notices information about computer games. Ben doesn't quite get it. Nothing he has seen so far interests him at all. Marketing messages can also be sent to consumers' hand held devices when they are in the vicinity of particular stores.

---

[226] The joining up of databases will have some possible positive effects – instead of the inconvenience and possible more serious consequences of suffering credit card cloning with weeks of investigation, it may be possible to resolve these crimes much more quickly, as with the example here.

[227] These full-body scanners come in several forms and are already being piloted, for example, the low-level X-ray-based Secure 1000 from Rapiscan: http://www.rapiscansystems.com/sec1000.html , tested at Heathrow airport, see: Lettice, J. (2004) ''See through clothes' scanner gets outing at Heathrow', *The Register*, 8 November, http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/ ; and the millimetre-wave scanners being developed by QinetiQ, and tested by Eurotunnel: http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html .

[228] Research on CCTV control rooms in the 1990s showed operatives used equipment for all kinds of inappropriate sexist behaviour – a technology that allows such intimate imagery is likely to attract similar problems. McCahill, M. and Norris, C. (1999) Watching the workers: Crime, CCTV and the workplace. In: Davis, P., Francis, P. and Jupp, V. (eds.) *Invisible Crimes: Their Victims and their Regulation.* London: Macmillan.

[229] 'Normalisation' at work, or the 'chilling effect' of a surveillance society.

[230] But on the other hand, surveillance can provide protection or redress against harassment.

[231] The origin of the term 'brandscape' is defined by the UK Design Council as the 'The total experiential reach and engagement of a brand. A term that encompasses all those who touch and interact with the brand including customers, suppliers, employees, competitors, re-sellers, distributors, partners, etc': http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPJLjJbFNakH0E0GQvlo&Document%5B@id%3D5232%5D/Chapter/@id=7 .

30. Cashless Shopping

30.1. The shopping centre then mines the data to find consumers who are the most frequent users of the shopping centre to offer them membership in their 'cashless' scheme. The scheme enables more 'valuable' consumers[232] to get an implanted chip to help them shop.[233] It costs £200 to get implanted. Then, consumers can load the chip with money, and pay in the different stores by getting their arm scanned rather than use a credit, debit or store card. The marketing for the cashless system tells shoppers that, as chip wearers they are eligible for discounts at stores of their choice in the shopping centre,[234] which will soon redeem the initial money paid for the implant. They also get access to a VIP lounge, spa and massage facilities on site, and they are less of a target for muggers or pickpockets, and even credit card fraud.

30.2. There have been rumours of shoppers being mugged in the car park and having the chips cut out of their arms, but the centre managers have dismissed theses stories as an 'urban myth'. Gareth considered joining up, but was worried as he had seen a television programme about the chips having only low level encryption and being in danger of corruption by viruses.[235] Chipping is however preferable to using a credit card for another reason. The consequences of being called about 'patterns of unusual activity' on one's card are now much more serious. Because of more sophisticated predictive algorithms based on individual consumer profiles, being called by the bank is now understood to imply guilt. Cards are automatically deactivated, and the consumer is required to provide independent evidence of their identity and location to the bank. The shopping centre takes a dim view of information requests from shoppers for this purpose.

31. Keeping Tabs on Kids

31.1. By 2016, mobility tagging and tracking have become a critical part of education.[236] Following a series of high profile cases in which pupils were either lost, injured or killed, many primary schools and even nurseries, became very concerned with keeping tabs on the whereabouts of their pupils to avoid legal liability.[237] Within ten years more and more schools adopted drug testing, in response to government policy aimed at identifying problem children early, tackling poor attendance and improving concentration in class – important in the face of the ever-present league tables.[238]

31.2. The cashless card system in Toby's school took off, with most families using it as a way of monitoring what their children ate. After three years, NSC, the supermarket, bought the cashless card company, seeing it as a way in to lucrative youth markets, building brand awareness by providing educational equipment. To get the resources, the parents are now required to swipe their child's card at the checkout, which identified the school, the pupil and the parent. The scheme funds computer equipment, science equipment, musical instruments and sports equipment for participating schools, providing their parents shop at NSC. The amount of

[232] The most valuable are determined by a credit check and reference to their consumer profile. Being a valuable customer means that you are likely to spend more. Implants become a status symbol.
[233] See Baja Beach (nd.) 'Zona VIP,' http://www.bajabeach.es/ .
[234] This will enable the database to record further individuals particular choices
[235] See: Rieback, M.R., Simpson, P.N.D., Crispo, B. and Tanenbaum, A.S (2006) 'RFID Viruses and Worms,' Department of Computer Science Vrije Universiteit Amsterdam, http://www.rfidvirus.org/ .
[236] It is now in an embryonic form in the USA. See, e.g: Leff, L. 'Students ordered to wear tracking tags', *Associated Press*, 9 February 2005, http://www.msnbc.msn.com/id/6942751/ .
[237] See e.g.: 'Neglect ruling in girl pond death', *BBC News*, 23 March 2006, http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm .
[238] In the UK, educational league tables rank schools according to the exam results of their pupils.

resources donated depends on the value of the parent's purchase. Some of NSC's key suppliers from the food and drink conglomerates have begun to install their vending machines in schools. Toby's school has continued with the scheme, and every time some new equipment arrived, the prominent 'NSC' brand could easily be seen.

31.3. The card has other uses too. The local education authority monitors the types of food being consumed in Toby's school, and uses it to inform various 'healthy eating' campaigns. The campaigns are also part of the authority's response to the Department for Education's Citizenship education programme. This is because the card has gradually became more integrated, not only holding data on the child's meal purchases, but also on their attendance, record of achievement, extra curricular activities, drugs test results, and Internet access. Records from the database attached to the card are submissable as evidence of students' citizenship activities. Whilst the increase of surveillance in schools has brought measurable benefits to the schools and pupils themselves, children are gradually becoming socialised into accepting body surveillance, location tracking and the remote monitoring of their dietary intake as normal.

32. Total Social Solutions?

32.1. In 2016, residential areas are more clearly divided between gated private communities, like that where the Jones family live, patrolled and monitored by well-equipped corporate security firms, and former council estates and low-cost housing like the Dobcroft Estate. For the Joneses, the camera and identification systems in and around the community keep insurance costs to a minimum.[239]

32.2. On the Dobcroft Estate, Yasmin's work is never done. Her multi-agency team has now been subcontracted to yet another private consortium called 'Total Social Solutions'(TSS). TSS is paid to monitor and enforce the multi-level Personal Behaviour Schemes[240] of which everyone on the Dobcroft Estate is a 'customer' from birth[241] (and some are identified even before[242]).

32.3. Many of those on higher levels of PBS[243] like Wilson Green, have RFID implants which register automatically with sensors installed in their homes and at the entrances of the estate.[244] The implants are supposedly voluntary, but like the schemes in shops and schools, compliance brings rewards, not least of which is earlier removal from the probationary scheme.

32.4. At the moment the whole Dobcroft Estate is also subject to one of its periodic 'area wide curfews' after 'youths' from the estate were supposedly identified by an

[239] The Association of British Insurers (ABI) has called for this in a major report on housing. ABI(nd) *Securing the Nation: The Case for Safer Homes*, London: ABI, 12.
http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf
[240] It is envisaged here that Anti-Social Behaviour Orders and Intensive Supervision schemes etc. (see Crime and Justice Expert Report) have all be standardised into general Personal Behaviour Schemes for those fitting certain patterns of risk of offending. Since all the residents of the Dobcroft Estate fit at least one criteria by the very fact of living on an estate where crime is likely to occur they are all subject to PBSs.
[241] See n.191.
[242] So-called 'biocriminology', or the genetic aspects of criminal behaviour, are enjoying a revival of interest at the moment; see e.g.: Rose, D. (2006) 'Lives of crime', *Prospect* 125(August), http://www.prospect-magazine.co.uk/article_details.php?id=7604 . For an earlier critique of this approach, see: Rose, N. (2000) 'The biology of culpability: pathological identity and crime control in a biological culture', *Theoretical Criminology*, 4 (1), 5–34.
[243] By 2016, prison is now just another level of PBS. Social work, probation and prison are all now a continuum, and largely privately managed.
[244] Supposedly to improve security for the residents, the Dobcroft Estate was fenced in 2010, leaving only four entrances and exits, which are monitored by Community Support Officers, cameras and RFID scanners.

elderly woman from the Sunnyview Retirement Village (where Geeta also lives) as causing trouble. The woman spotted the suspicious activity on the local video surveillance cameras. The cameras can be watched on the local security channels on digital TV, which also includes a 'rogues' gallery' of those who have known to have infringed their PBSs.[245] In residential areas, public area CCTV has almost entirely become Open-Circuit Television (OCTV). All under 18s are currently barred from entering or leaving the Estate from 6pm until 6am. For Sara, this means that to see her best friend, Aleesha, outside school hours, one of them has to risk an encounter with the estate's Community Wardens, who are armed with tazers and tend to shot first and ask questions later.

33. Driving Change

33.1. When Gareth drives out of the community, the wrought-iron gates swing open automatically, and his number plate is read, noting his exact time of departure, and the number and identity of the driver and passengers. On the roads, ANPR has been nationwide since 2008 and there are now so many cameras there is no point in trying to second-guess where they are with scanners or maps any more.

33.2. In any case, the handheld computer that Gareth plugs into his car[246] is linked to the Galileo global satellite navigation system[247] and to state congestion cameras, and helps provide the quickest route. Finding the shortest route is also less expensive as through the ANPR system, car mileage is automatically charged to Gareth's bank account.[248]

34. Friendly Flying Eyes in the Sky

34.1. Like the border, the shopping centre and school, the wider city of 2016 is at once more under surveillance yet sometimes less obviously so at an immediate glance. Security has been aestheticised; designed into many of the buildings and surveillance is built into the infrastructure and architecture – it is ubiquitous but has disappeared.[249] Many important state buildings which had been surrounded by concrete barricades after 2001, now appear open once again, but are instead protected by a variety of sensors linked to impenetrable automated barricades that sink into the ground when not immediately needed.

34.2. When Ben and Aaron go into the centre of London to join an anti-war protest they are monitored by small remote-controlled spy planes, Unmanned Aerial Vehicles (UAVs).[250] These were introduced for the Olympics of 2012, but instead of being withdrawn afterwards, the 'success' of these 'friendly flying eyes in the sky'

---

[245] Such a scheme was introduced as an experiment in Shoreditch in London in 2006. It was immediately dubbed 'ASBO TV', see e.g.: Swinford, S., 'Asbo TV helps residents watch out', *Times Online*, 8 January 2006, http://www.timesonline.co.uk/article/0,,2087-1974974,00.html .

[246] In 2016, most people now have these devices which incorporate roaming wireless Internet access, telephone services, computer navigation and more. The navigation function also ensures that the devices (and therefore their operators) are trackable.

[247] Galileo is the European civil alternative to the US military GPS system. The first satellite was launched in 2004 and some services will be operational by 2008, see: 'Galileo, European Satellite Navigation System' CEC Directorate General Energy and Transport, http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm .

[248] There are many potential schemes. See .e.g.: Independent Transport Commission (2006) *Paying to Drive* http://trg1.civil.soton.ac.uk/itc/p2d_main.pdf .

[249] See: Infrastructure and Built Environment Expert Report.

[250] UAVs have been in use by the US military for some years: currently the best-known example is the 'Predator' reconnaissance drone aircraft used in Iraq; see: 'Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA', *airforce-technology.com*, 2006, http://www.airforce-technology.com/projects/predator/ . Many uses have been suggested in the UK, see: Jha, A.,'On the horizon ... pilotless planes as fishermen's and firefighters' friends', *The Guardian*, 30 August 2006, http://www.guardian.co.uk/science/story/0,,1860825,00.html . In Los Angeles police are already experimenting with small remote control spy planes called 'SkySeer': Bowes, P., 'High hopes for drone in LA skies', *BBC News*, 6 June 2006, http://news.bbc.co.uk/1/hi/world/americas/5051142.stm .

as the government has dubbed them,[251] has been hailed by the Mayor as a reason for their continued general use.[252] People have almost stopped noticing them now.

34.3. CCTV is also less noticeable. Smaller cameras are embedded in lampposts at eye-level and walls, which allow the more efficient operation of the now universal facial recognition systems.[253] Morphing software which combines images from multiple cameras to build a 3-dimensional picture is also being pioneered, although campaigners and lawyers argue it is inaccurate and not a 'real' image.

34.4. It is not just the cameras themselves. Almost universal wireless networking allows the cameras to be freed from bulky boxes and wires. In addition, the cameras are linked to intelligent street lighting which provides 'ideal' lighting conditions for recognition software, and also movement activated floodlighting and extra cameras in the case of crowd 'clumping' or unusual movement.

35. The Unidentified Underclass

35.1. After the protest in 2016 Ben and Aaron are stopped by private security employed by the Westminster Business Improvement District.[254] The guards are remotely supervised by police operators via their handheld computers[255] and helmet-mounted microcameras, which scan the two boys.[256] Ironically it is the police and security officers themselves who have been most concerned about the continuous monitoring as it means they are under constant scrutiny and feel they have lost 'flexibility' of response.

35.2. Ben submits to the usual DNA swab, which is now analysed instantaneously, and hands over his ID card, which is scanned. As the data flicks up on his screen, the officer jokes that it seems ironic that an anti-capitalist like him has just been on holiday in the USA.[257] Ben grimaces politely.

35.3. ID cards are still supposedly voluntary and Aaron, who comes from a Christian family, refuses to have one. His mum says it is 'the mark of the beast', but he just wants to be left alone. He's finding it hard now though: not having a card means he has effectively opted out of the chance to apply for government jobs, receive benefits or student loans and he can't travel by plane or mainline train even within Britain. He's beginning to wonder if it's worth it and how he can live: he's heard about cooperative projects in the countryside where people live without ID, but he's a city boy and he's afraid of 'dropping out'. It's about to get worse for him: as a young

[251] 'The friendly eye in the sky' was how CCTV cameras were referred to by a Home Office minister as far back as 1995, see: Campbell, D. (1995) 'Spy cameras become part of the landscape,' *The Guardian*, 30 January: 6.
[252] Major sporting events have had a history of being used for the testing and introduction of new surveillance technologies. For instance, on CCTV and the 2002 World Cup in Japan, see: Abe (2004) *op cit.*, n.161; and on CCTV and the Athens Olympics, see: Samatas, M. (2004) *Surveillance in Greece*, Athens: Pella.
[253] See Crime and Justice, and Infrastructure and Built Environment Expert Reports. One of the big problems with facial recognition had been the angle of view of CCTV cameras; see e.g.: Introna, L. and Wood, D. (2004) 'Picturing algorithmic surveillance: the politics of facial recognition systems', *Surveillance & Society*, 2(2/3): 177-198.
[254] Urban governance is already being turned over to Public-private partnerships, Town Centre Management organisations http://www.atcm.org/ and BIDs. According to the government, BIDs provide "an investment in the local trading environment through the provision of added value services" http://www.ukbids.org/ In 2016 one of the biggest regulation issues is information sharing between state and private security firms acting on behalf or instead of the state, especially now the Police Naitonal Computer links so many databases together, and that police, probabiton, pison and social services are so interconnected.
[255] Many police services are already trialling these, see e.g.: 'Pocket computers put police 'in the picture'', *West Yorkshire Police*, 28 March 2006, http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226 , and the 'Airwave' scheme (see Crime and Justice Expert Report) is designed to build them in.
[256] Again, helmet cameras linked live to control rooms are being introduced in several areas already; see e.g.: 'Police use anti-yob head cameras', *BBC News*, 23 March 2006, http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm .
[257] The police and their private allies have access to just about every database now linked by the Police National Computer.

black male with no ID card, he is highly categorically suspect and the police control room instructs the security personnel to bring him in for extra questioning.[258]

36. Virtual Tracking

36.1. After Ben is let go by the police he heads home to Finchley, but his own handheld computer is now being tracked via the Galileo system[259]. He has also put on a watchlist for communications monitoring: his ISP has been served an automated RIPA 2 order that all his Internet traffic and e-mail communications are saved and passed to police.[260] As most telephony is now conducted over the Internet, and old landlines are disappearing, this covers all Ben's communications.

36.2. One of the consequences of this and the continued 'ownership' of the Internet by US-based companies has been renewed efforts by the Open Source movement, and also by other powerful nations to create 'alternative Internets'. By 2016, these include a much more controlled Chinese language project[261] that now covers much of South-East Asia, several transnational corporate ventures including the 'Googlenet'[262] and many more libertarian and 'transparent' 'Net projects.[263]

36.3. One unforeseen result of the surveillance of Ben's communications is that Ben's younger brother Toby, who occasionally uses Ben's accounts (largely just because he enjoys cracking) is also drawn into the monitoring. Toby lives a lot of his life online in 2016, in Massively Multiplayer Online Games (MMOGs): virtual worlds that have their own rules and entire alternative economies.[264]

36.4. The surveillance society has already spread here too. Players' behaviour in the game[265] is monitored by companies who aim to understand the new opportunities for emerging real-life markets. A whole new class of corporate game player has emerged. These players research the habits of people via their avatars and market both virtual and real products inside and outside these worlds to other players.[266]

36.5. Police have also begun to experiment with software also monitors MMOGs to identify avatars who exhibit certain types of behaviour that could indicate real-world

---

[258] In 2016, there are still arguments in the media and politics around the police doing this. But they argue that ID cards provide an easy way of determining someone's bona fides, and they cannot take the risk oaf assuming the innocence of people without one.

[259] See n.247.

[260] The current Regulation of Investigatory Powers Act (RIPA) 2000 allows limited record retention, but we assume that police and security services will want remaining 'loopholes' closed, most probably in response to a some highly publicised scandal connected to terrorism or paedophilia, and achieve this with a new RIPA in 2009.

[261] This has been under development for some time, see: 'China to launch 'alternative' Internet,' *New Scientist Technology Blog*, 1 March 2006, http://www.newscientist.com/blog/technology/2006/03/china-to-launch-alternative-internet.html

[262] Reports have been circulating since 2005 of Google's ambitious plans in this direction, see e.g: Hedger, J. (2005) 'Is Google building an alternative Internet?' *SiteProNews* 23 September, reprinted: http://www.wnwdesign.co.uk/wordpress/archives/197

[263] See e.g.: Brin, D. (1999) *The Transparent Society*, Reading MA: Perseus. http://www.davidbrin.com/tschp1.html

[264] MMOGs, by some estimates, currently have around 13 million subscribers, with the largest being *World Of Warcraft*, http://www.worldofwarcraft.com/index.xml , and the Korean game family, *Lineage I*, http://www.lineage.com/ , and *II*, http://www.lineage2.com/ . Other virtual worlds are more like analogues of the real world, and include *Second Life*: http://secondlife.com . They are becoming increasingly immersive and their economies intersect more and more with the real world, with items from the games being traded for 'real' money on auction sites such as *ebay*, http://www.ebay.com . See *MMOGCHART.COM*, http://www.mmogchart.com/ for some statistical analysis.

[265] Residents of virtual worlds are usually represented by an 'avatar', an online character.

[266] There have already been some accounts of 'virtual surveillance'; see e.g.: 'Confessions of a Virtual Intelligence Analyst', *Terranova*, 15 March 2006, http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html . Marketing analysts have already identified significant emerging virtual markets which means that companies are starting to target game worlds, see e.g.: Burns, E., 'Marketing Opportunities Emerge in Online Gaming Venues, *ClikZ*, 1 August 2006, http://www.clickz.com/showPage.html?page=3623035 , and the first 'virtual billboards' have already been launched, see: Shields, M., 'Massive Unveils Toyota Ad Units Within Anarchy', *Mediaweek*, 19 July 2006, http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380 .

criminal tendencies in their players.[267] This of course is hugely controversial amongst gamers who argue that the escapism of virtual worlds should not be mistaken for real life.

37. Your Life is Our Business

37.1. The call centre of 2016, in some respects, is identical to the call centre of 2006. Employees are still monitored every minute of the day, via a computer which records every activity they perform, how long they perform it and how well they do so. Methods of employee recruitment and reward are very different, and characterised throughout with surveillance techniques which Gareth has had to get to grips with.

37.2. During recruitment, employees are now subject to a range of biometric[268] and psychometric tests, and lifestyle surveys. Their lives outside work, and their background are the subject of scrutiny. It is felt to be increasingly important that the lifestyle profile of the employee match those of the customers to ensure better customer service.[269] Frequently, prospective employees are apprehensive about the health tests, and so have begun, on the advice of the recruitment agencies that supply the call centres, to volunteer their health information to avoid the tests. To save time, recruitment professionals now regularly discard CVs without volunteered health information.

37.3. Gareth is also a firm believer in the ongoing management of employee well-being. After all, how is a management team to know anything about what is making their employees tick by simply using a set performance statistics?[270] For example, periodic biometric testing alerts the employer to any health problems, and also signals whether the employee needs counselling.[271] In conjunction with a local gym, which also has the same iris-scanning access control system as the call centre, employees can exercise for a reduced entry fee. Their gym attendance shows up on their electronic employment record. Employees who do not attend the gym regularly are sometimes questioned about their lifestyle in their annual appraisals, particularly if their performance at work has been below par. Periodic psychometric testing also indicates to management whether the employees' attitudes are thought to be compatible with company values and culture.

37.4. Call centre work has bifurcated: the most simple queries and administrative tasks have been automated or outsourced offshore. However some call centre jobs now involve incredibly complex personal sales work. With Reward Card data consortia amalgamating and selling detailed information on consumer profiles, call centres are able to provide an integrated service to their most valued customers. When a customer rings for service on one product the employee's desktop displays the entirety of the customer profile. The employee is then able to ask the customer about other products, perform online credit checks and offer discounted rates there and then. With so much information on the individual consumer to hand, Gareth calls this style of selling 'customer intimacy'. He believes it is the way forward for

[267] This was following a number of incidents over several years featuring spillover incidents from MMOGs and real-world crime; see e.g.: 'Chinese gamer sentenced to life', *BBC News*, 8 June 2005, http://news.bbc.co.uk/1/hi/technology/4072704.stm .
[268] Biometric testing, which involves mouth swabs and urine samples, easily analysed by the on-site nurse using a cheap kit, means that the employer can assess whether the prospective employee poses any productivity risk, as the test alerts the employer to potential health problems. It also enables the organization to design a flexible benefits package around the individual employee, assigning different values to the health insurance component depending on the employee's state of health.
[269] A downside of this is that an organization would only employ a particular type of person, and thus have a less diverse workforce, see: Workplace Surveillance Expert Report.
[270] This statement is intended to highlight how management are involved in an ongoing push to 'measure the unmeasureable' – work processes, attitudes, health and culture.
[271] For example, for alcoholism if their blood alcohol levels are too high, as indicated by a urine test.

call centre work, providing a more rewarding job for the employee, and a more personalised service to their most valuable customers.

38. Looking After You

38.1. The Sunnyview Retirement Village is a rebranded and privately-managed set of council flats in which 74-year old Geeta has lived for some years. She feels very reassured even though she lives alone, because of her full participation in the local 'Telecare' scheme. In addition to motion detectors in every room, her bath has an inbuilt heart rate monitor, her toilet has an device which measured her blood sugar levels, and her kitchen had a number of sensor which detect gas leaks, fire and floods. She has a panic button linked to the local authority call centre, which will instantly call and check on her if it is pressed.

38.2. The presence of sensors and cameras all over her home means that her family know she is safe and she gets fewer family visits than she use to, which leaves her feeling a little isolated. However, she finds the RFID scanners in her fridge and cupboards extremely useful. Every time she is running low on groceries, her household management computer orders products from her local NSC supermarket over the internet. Her subscription to home delivery means that she does not need to make unnecessary visits to the shops.

38.3. By now, she is also used to her regular 'Well Woman Checks'. She has even got to know the nurse, Anita who was the daughter of one of her neighbours. The check features the similar tests to those of 2006: blood and urine samples are taken, and her height, weight, blood pressure and eyesight are checked. Luckily Geeta is in good health.

38.4. However she is not party to the massive changes in health screening that have been taking place behind the scenes. Unknown to her, the hospital which analyses her results now routinely uses computer vision to analyse mammograms, and with the huge development in patient databases, Geeta's results are compared to those of other women her age from every other health authority in the country.[272] The database also enables health professionals to hone in on risk factors surrounding many of the diseases for which she is screened, so the statistical likelihood of her actually suffering, for example, a heart attack, is predicted with a much greater degree of accuracy. Her local Well Woman Clinic is continually providing Geeta with dietary advice, as she is in a high risk group for heart disease.

38.5. This is also true for many other risk categories relating to common diseases. Lines of statistical causality are being drawn between a much wider range of ailments and their indicators. Larger proportions of the population are routinely being categorized and screened, which helped the statistics. Yasmin often complained about the number of times Gareth misses his 'Well Man Check' because, like many men, he is so reluctant to go to the doctors. She wonders how many other people like him take the persistent screening requests seriously.

38.6. Health service statisticians are also keen to get hold of consumer data to support their hypothesis that diet has a big role to play in the nation's health. However they are having difficulty. With the national patient database now developed and working properly, the NHS is continually refusing insurance companies access for health information on a 'need to know' basis, despite the huge temptation it has to make

[272] See, e.g.: 'The future of screening', *BBC News*, 14 December 2002, http://news.bbc.co.uk/1/hi/health/2570787.stm .

large amounts of money from doing so. As such, NHS bosses feel unable to ask for access to private consumption information as a matter of principle. They are still haunted by the scandal in Iceland, which sold its national DNA database information to private companies for research and private profit.[273]

39. Conclusion: The Hall of Mirrors

39.1. Whilst surveillance is more pervasive in 2016, citizens, and particularly those educated or wealthy enough to appreciate or afford it, are increasingly aware of it and able to find new ways of negotiating their own personal economy of information. Gareth is signed up to a personal information management service that monitors his 'data shadow' online. This automatically corrects incorrect information held on public and some consumer databases and which alerts him to further problems.

39.2. Unfortunately not everyone is able to change and access their personal information equally. Those less skilled in personal information management or less able to pay for others to manage their information for them are at a severe disadvantage. The ability of devices to block these messages (which are inbuilt in the more expensive models) is critical to those who are privacy-aware and wish to make relatively independent choices about consumption.

39.3. The digital divide has grown ever deeper with the some condemned to a purgatory of surveillance and an inability to access information. Open Source campaigners have managed to make it far easier to access and change personal information held by the state and private companies working for the state, but this access is one of the many things now made conditional on having an ID card. There is an increasingly uneasy and as yet unresolved stand-off between citizens and the state about who knows what, who owns data and who has the right to change data.

39.4. But in 2016, people are more used to watching and being watched. Many voluntarily carry out whole life surveillance, or life-logging, recording almost everything they do and storing it or placing it straight online[274] in real-time. What was a subculture in 2006 is starting to become mainstream in 2016.

39.5. However the culture of peer-to-peer surveillance has also splintered and produced new variants. There is a great deal of vigiliante surveillance by hardliners who feel that the state is 'not doing enough' to control terrorism, crime and illegal immigration,[275] and unofficial websites of the 'suspect' have proliferated, leading to all kinds of mistakes and misidentifications.[276] Protestors, artists and surrealists all play with and resist pervasive surveillance in all sorts of ways, including disabling public surveillance devices,[277] using 'sousveillance' technologies or counter

---

[273] McKie, R., 'Icelandic DNA project hit by privacy storm', *The Observer*, 16 May 2004, http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html . See also: Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database*, London: The Wellcome Trust. http://www.mannvernd.is/greinar/hilaryrose1_3975.pdf

[274] Life logging of Life Blogging is developing out of Web logging (blogging). Many technologies are already being developed to support it; see e.g.: Ward, M. (2004) 'Log your life via your phone', *BBC News*, 10 March, http://news.bbc.co.uk/1/hi/technology/3497596.stm .

[275] See the Borders Expert Report, and e.g.: the US Minutemen border security vigilantes: http://www.minutemanproject.com/

[276] This has already been noted in connection with the panic over paedophiles that resulted in a paediatrician being driven out of her home in 2000, see e.g.: Allison, R., 'Doctor driven out of home by vigilantes', *The Guardian*, 30 August 2000, http://www.guardian.co.uk/child/story/0,7369,361031,00.html . We simple assume that in 2016, technologies will allow such errors to circulate faster and more widely.

[277] Guides to such resistance already proliferate; see e.g.: 'Guide to Closed Circuit Television (CCTV) destruction', *Schnews*, http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisioncctvdestruction.htm .

surveillance.[278]. Anti capitalist activists like Ben and Aaron, for instance, like to spend their Saturday afternoons slapping highly adhesive aluminium sheeting and tiny battery powered microwave transmitters to the entrances of shops to disrupt the wireless signals.[279]

39.6. Life logging is also not all that is can seem and with increasingly sophisticated data management and video production software, lives can be adjusted or even entirely created for purposes from pure entertainment through subversion to fraud. For example, Toby has an alternative data shadow that a sophisticated cracker friend of his has created is several years older than him and significantly more exciting and better looking! And in 2016 there are increasing numbers of entirely virtual data shadows, who have no real world counterpart, who appear to exist and are themselves the subjects of information management and online surveillance by automated systems working quietly and invisibly, inhabitants of an endless hall of mirrors…

[278] See Mann, S., Nolan, J. and Wellman, B. (2004) 'Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & Society*, 1(3), 331–355.
[279] RFID is a line-of-sight technology. Interference can be achieved with microwaves, sheet metal, brick and even tree sap, see e.g.: 'RFID Technology', *RFID Centre*, http://www.rfidc.com/docs/rfid.htm .

Part D: Regulating the Surveillance Society

40. Introduction

40.1. As we have seen in Part C, the Jones family are under surveillance every day, and in a large number of events and activities, and could be far more integrated in surveillance processes in 2016. Some of the surveillance processes are benign or helpful to them; others have more ominous or exploitative implications for a host of values and interests that the Joneses, as ordinary citizens, hold to be important, and that their country holds as important to its idea of a good life in a democratic society governed democratically by the rule of law. For a great deal of the time, the Joneses do not know, or understand, what happens or can happen to their personal information: what is being collected, processed, sorted and communicated. Most of the time, these are not matters of concern to them; but sometimes, things begin to go wrong for them, and they suspect that something has happened to their information to bring about adverse consequences. What do they think can be done about that? What *can* be done about it, and by whom, if not the Joneses? What keeps surveillance within legitimate bounds? How can these controls be improved, in order for regulation to keep up with the Joneses?

40.2. Surveillance requires regulation. By 'regulation' we do not mean only legal devices for controlling systems and practices, but any techniques that have a regulatory effect[280]: that is, they apply rules, one way or another, to surveillance or the processing of data by setting limits and controls. This may sometimes involve facilitating 'good' surveillance by governing it within a framework of principles, rules and required safeguards, whilst proscribing activities that do not submit to the technique or regulatory regime. Most of the systems for controlling information processes concerning personal data have been developed in the context of data protection, with the aim of safeguarding *privacy*. Our comments in this section deal mostly with these strategies. But regulating *surveillance* could be something else again. Privacy protection might be the first line of defence against the undesirable effects of surveillance. As such, it is not without strength and resilience, despite much contemporary hand-wringing about its impotence and finger-wagging about its supineness. On the other hand, it could be argued that surveillance protection must be devised in its own right, because its undesirable effects are not only those that have to do with the invasion of privacy, and that the first line of defence, though not negligible, is vulnerable. We believe that both of these positions are valid in theory, and that, in practice, surveillance protection is highly likely to coincide with, and to borrow from, the experience and infrastructures of privacy or data protection. Yet, as is shown in this Report's discussion of the regulation of telecommunications, the effectiveness of conventional rules of protection is a serious problem in regard to certain applications and crucial technologies. How much invention is necessary for surveillance protection, and how much of that would actually be re-invention, is a matter for extended discussion beyond this Report, although we return to it below in

[280] Baldwin, R. and Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press.

our discussion of privacy impact assessment. So, too, is the question whether the regulation of surveillance is really possible.

40.3. The surveillance practices that have been canvassed elsewhere in the Report point up the implications for privacy and a host of other important values: justice, dignity, self-determination, social inclusion, security, and others. Many of these values can be safeguarded if privacy is safeguarded. Some forms of surveillance enhance the ability of individuals, groups and societies to realise these, and are thus consistent with what most people would expect of life in democratic countries where human rights and liberties, as well as collective interests, are respected. On the other hand, many surveillance practices threaten these values through the adverse effects they have in a host of settings: at home, at work, in public spaces, in citizens' relations with the state, in shopping, at borders, in physical movement, and so on. The risk of privacy invasion is commonly, but not necessarily, involved in these practices. New technologies, and new uses for older ones, hold promises as well as pose dangers, and future implementation of developments – for example, in ambient intelligence and ubiquitous computing – may have implications that we can only guess at. Our scenario relates existing surveillance practices to the life of a fairly typical family going through a fairly routine week in their lives, and our vignettes project forward several years. But they do not show the effects of regulation upon surveillance or privacy invasion, even though that is the subject of a great deal of regulatory activity in many countries, and at international levels and in a range of organisations within and among states. Many would argue that these effects are likely to become weaker, and even that regulatory systems and strategies are doomed to fail unless – or even if – they are overhauled.

40.4. This section of the Report addresses these issues. We reflect on the regulatory experience, and assess the adequacy of these efforts. We are mindful that measuring the effectiveness of privacy protection and of the regulation of surveillance is a highly debatable undertaking,[281] but if this Report stimulates such debate, it will have achieved one of its purposes. We also suggest possibilities for improvement.

41. What is Wrong with Regulation?

41.1. It may not be wide of the mark to say that regulation and the context of discussion about privacy and surveillance, in any country, has suffered from some common drawbacks. In pointing these out, we are implying no criticism of any one country or of any participants in regulation; much less are we aiming to construct an international 'league table'. However, we are able to identify at least six areas of difficulty of a general and contextual kind:

- Regulation has tended to be reactive: that is, response had been made to technological development, implementation and practice after the fact.
- Regulation has had a largely technical and managerial focus, based on codes of practice, the fulfilment of standard legal requirements, and the application of privacy-protective technologies, leaving little room for anticipation.
- Much regulation has been based on a narrow conception of personal privacy and of its value to individuals alone, (necessarily) reflecting the current thinking of policymakers who often implement a restricted view of what is in the 'public interest'.
- Regulation has been discussed and implemented largely outside of public debate. Debate has taken place within expert communities: for example, the world of data

[281] Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge MA: MIT Press, ch. 9.

protection or law-enforcement. This has meant very little engagement amongst ordinary people with some of the most important issues of our time.

- Regulation is often seen, in political terms, as a burden unfairly placed on business as well as the state, inhibiting initiative, risk-taking and productivity. In Britain, there has been a marked attempt at deregulation, or 'better regulation', to lighten the load. Along with health and safety and environmental implications, privacy protection and checks on surveillance are caught in this net, making it difficult for new or more exacting requirements to be implemented. The recognition that business and government may stand to benefit from the public-trust and efficiency gains that regulation may bring is very patchy in practice, although more evident in rhetoric.
- Media discussion concentrates heavily on 'horror stories' about incidents of privacy invasion, and also portrays both utopian and Orwellian views about surveillance technologies. Newsworthy stories are important, but too often, the complex ethical and social issues around surveillance are ignored. When surveillance is discussed, it is often in terms of either simple cause-and-effect ('CCTV will prevent crime') or fear ('we will all be under control'). Similarly, alternative views are countered by the fallacious and dangerous argument that 'if you have nothing to hide, you have nothing to fear'.

41.2. These are among the main general and contextual difficulties that can be highlighted in today's regulatory environment; later on, we will comment on problems with specific regulatory mechanisms Some of the general difficulties and circumstances may be amenable to change, although with difficulty; others may not. Yet the world of surveillance and privacy regulation has been far from inactive, and its efforts have not been in vain, although serious doubts exist over the record of past achievement and the prospects for the future.

42. The Current State of Regulation

42.1. For the past thirty-five or more years, privacy protection has spread round the world as a response by countries and international bodies to perceived threats coming from public and private sector activities that often have at their disposal sophisticated technological means for processing personal data.[282] Lying at the heart of these developments have been some totemic principles, contained in a variety of wordings in many laws and official documents. They require that an organisation:

- must be *accountable* for all the personal information in its possession;
- should *identify the purposes* for which the information is processed at or before the time of collection;
- should only collect personal information with the *knowledge and consent* of the individual (except under specified circumstances);
- should *limit the collection* of personal information to that which is necessary for pursuing the identified purposes;
- should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the *finality* principle*)*;
- should *retain* information only as long as necessary;
- should ensure that personal information is kept *accurate, complete and up-to-date*;
- should protect personal information with appropriate *security safeguards*;

[282] 'Processing' is defined here in accordance with Article 2(b) of the European Data Protection Directive 95/46/EC to mean: 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collecting, recording, organizing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

- should be *open* about its policies and practices and maintain no secret information system
- should allow data subjects *access* to their personal information, with an ability to amend it if it is inaccurate, incomplete or obsolete.[283]

42.2. Imbued with these or similar sets of 'fair information principles' (FIPs), the regulatory world for governing privacy invasion and surveillance has been populated by general laws, laws covering certain sectors (e.g., telecommunications) or practices (e.g., data-matching), and international documents and declarations at the global and regional level, of which perhaps the most prominent is the European Data Protection Directive 95/46/EC, also reflected in the Telecommunications Directive (97/66/EC). Regulatory authorities such as privacy and information commissioners have been established at national, sub-national, and even regional levels, In addition, private companies, trade associations, and public authorities have formulated their own codes of practice and protocols, and online merchants have adopted privacy statements or policies. In certain countries, non-statutory confidentiality rules and laws have governed the surveillance practices of professions and others who process personal data that are often highly sensitive. Penalties and sanctions have been applied to offenders under the various forms of legal regulation. In recent years, technological solutions – privacy-enhancing technologies, or PETs – have been enlisted in the cause of limiting collection, providing anonymity, and otherwise mitigating the surveillance potential of technology itself. Privacy advocates have been vocal and active in warning of dangers, exposing practices, and raising public awareness of how surveillance and privacy invasions may affect their lives. The media have often responded to surveillance's threats, even as the media itself finds it profitable to invade the privacy of celebrities and 'ordinary' citizens alike.

42.3. In sum, there has been much interest and activity concerning surveillance and privacy, and the community of persons and organisations involved in it is numerous and widespread. Yet much doubt remains that even the best efforts, and the principles itemised above, are weak in the face of the persistence and increasing sophistication of classical, routine privacy invasions in the business sector, more pervasive surveillance through the use of telecommunications technologies, and new government policies that are predicated upon the processing of personal information for a host of proactive, predictive approaches to solving social problems, based on the processing of vast amounts of personal information. As people increasingly move round the world – whether for business or leisure travel, or for immigration and asylum-seeking purposes, or to commit acts of terrorism – surveillance activities gain a heightened international, cross-border dimension that surpasses that of the past.

42.4. These developments have fed a self-fulfilling, and sometimes self-serving defeatism, expressed in the widespread attitude – cultivated by certain interests – that 'privacy is dead; get used to it', for it weakens the constituency of public, political and business support that regulation might otherwise enjoy, and that it needs. So too does the frame of mind that seeks always to balance the control of surveillance against the public interest in safety and security in an age of fear – a 'balance' in which the former is almost always bound to lose. The 'reasonable expectation of privacy', which has come increasingly to define the framework within which regulation is discussed and promoted, risks being deflated as people, including today's children – if, say, they are fingerprinted at school or for passport purposes,[284]

[283] *op cit.* n.281, 12.
[284] Doward, J. (2006) 'Millions of children to be fingerprinted'. *The Observer*, 30 July, http://observer.guardian.co.uk/uk_news/story/0,,1833407,00.html

monitored by interoperative government databases, or tagged by their fearful parents in order to track their comings and goings for safety reasons – 'get used to' more and more limitations on their freedom from surveillance.

42.5. This Report is not the place for an extended discussion of the underlying theories of surveillance that have been current over several decades. However, many of those who have been studying surveillance have tended to question the emphasis on privacy and its protection as the main arena in which surveillance is arbitrated, for privacy itself is but one of the values at stake, and in the conventional understanding is construed only, or mainly, in terms of individual rights and freedoms that are enforceable at law.[285] Building a practical system to control surveillance on the slender and perhaps battered foundation of information privacy protection seems, to many, to be misguided. To others,[286] however, privacy and its protection is capable of being extended to cover other, physically intrusive, situations in which there is an asymmetry between the individual and the surveillors, as in video surveillance. To take another example, the mobile tracking of workers and others 'on the move', using sophisticated surveillance technologies, can be, and to an extent already is, regulated by applying the classical principles to the practices of organisation and by employing a range of regulatory instruments – described later – in a vigorous and concerted way.[287]

42.6. We are not persuaded that, in searching for regulatory solutions to surveillance, the baby should be thrown out with the bath water; or, to change the liquid metaphor, that privacy principles and regimes are now, like King Canute, incapable of holding back a supposed flood of surveillance. The set of 'fair information' data protection principles is the only reasonably structured, systematic and practically oriented ethical framework currently available.[288] It is not credible to suppose that nearly forty years of privacy protection has been a delusionary game played by legislators, regulators and others who have focused on the wrong targets; or that those targets no longer present threats. Many successes in regulating surveillance by means of the privacy defensive perimeter can be credited to the existing protective regimes established in and among jurisdictions, although, to be sure, the record is uneven and the regimes are not all equally empowered. That said, it might be a delusion to suppose that the conventional wisdom of privacy and data protection and the practical measures to which it has given rise can still deal successfully with some of the present and much of the future. In that future, what has been called 'the new surveillance'[289], involving the latest suite of technologies, combines with elements of the 'old surveillance' based on the technologies of the 'computer age'. In a world of ubiquitous computing, for example, it is difficult to see how a number of privacy principles or fair information practices can be brought to bear effectively in a regulatory capacity; but their applicability should not be casually written off.

42.7. Moreover, new surveillance practices increasingly entail discriminations and other social 'bads' in ways that have powerful and inequitable effects upon life-chances beyond the realm of privacy violations themselves, which have consequences mainly for individuals. It is arguable, therefore, that the regulatory

[285] Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press; Lyon (2003) *op cit.* n.6.
[286] e.g.: Dubbeld, L. (2004) *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance.* Enschede: Ipskamp Printpartners.
[287] Bennett, C. (2005) 'Surveillance, employment and location: Regulating the privacy of mobile workers in the mobile workplace', in Hansson, S. and Palm, E. (eds.), *The Ethics of Workplace Privacy.* Brussels: P.I.E-Peter Lang.
[288] Bennett, C. (2006) 'The mobility of surveillance: challenges for the theory and practice of privacy protection'. Paper presented at the 56th Annual Conference of the International Communication Association, Dresden, 19-23 June, panel on *Individual and Social Perspectives of Online Safety*.
[289] Marx, G.T. (1998) 'Ethics for the new surveillance,' *The Information Society* 14 (3): 171-85.

regimes for surveillance and privacy need to be re-thought and modified (at least) to be able to affect the design, implementation, and effects of new, more intensive and extensive, surveillance technologies. But the new surveillance is not just about technologies. It can be claimed that the 'problem' for regulatory regimes is not only how to cope with the technologies, but also how to influence the policies and purposes of those who develop and deploy them, and how to influence societies and populations who are subjected to them.

42.8. Privacy, therefore, might not be dead, but the jury is out on whether privacy regulation, as we have known it for some thirty-six years, might be, when one considers certain novel threats. Therefore, 'new regulation' may well be needed, not as a wholly new social and governmental philosophy or practice, but as a reconstruction that incorporates what is still sound and resilient from the recent past. In 1998, Gary T. Marx[290] argued that the data protection model was no longer up to the job, and that it needed a more encompassing framework of ethical principles to cover more than just information privacy, and to cover surveillance in a more substantive way. These principles were implicit in the conventional model, but they needed to be brought to the surface and related to the means, contexts and uses of surveillance data. He propose some 29 questions to be asked in determining whether surveillance conforms to ethical principles; we will argue later that this determination has an affinity with privacy impact assessment (PIA). Whilst Marx did not systematically specify which of the data protection or fair information principles or practices were still relevant, which were not, and how they related specifically to his inventory of questions and the principles they embodied, they are clearly not, or not all, on the scrap-heap.

43. Regulatory Instruments: Pros and Cons

43.1. Let us briefly canvass, and comment upon, the existing repertoire of broad, partially overlapping, categories of policy instruments that have been brought into use for privacy and data protection, and therefore apply to large areas of surveillance as well:[291]

43.2. *International instruments*

43.2.1. The European Convention on Human Rights, and other international declarations, give legal and moral force to privacy protection that may play a significant part in reining in the excesses of surveillance. More specifically, the OECD,[292] the Council of Europe[293] and the EU[294] are among the most prominent contributors to the evolution of principles and rules for limiting surveillance and invasions of privacy, mainly with regard to information privacy. These and related documents have shaped specific legislative and implementation activity in a very large number of countries and lesser jurisdictions. Some of these international instruments have retained their moral force, although the value of this asset is now questionable. Nevertheless, action at the international level is largely responsible for the pre-eminence of the set of principles, already listed, that have governed data protection, and by extension, many of the practices associated with surveillance, for a long time.

---

[290] *ibid.*
[291] For a more detailed typology and discussion, see *op cit.* n. 281: chs. 4-7.
[292] OECD (1981) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD.
[293] Council of Europe (1981) *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).* Strasbourg: Council of Europe.
[294] Especially European Union (1995) *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Brussels: OJ No. L281, 24 October [The EU Data Protection Directive]

43.2.2. The principles that were referred to earlier are inherent in the 'privacy paradigm'[295] that we have inherited, and that is exemplified in most countries' approaches. It is mainly a derivative and procedural construction that somewhat obscures substantive, ethical considerations that lie in the background, although they are not out of sight. It enjoins upon 'data controllers' a set of largely procedural requirements for their processing activities, and therefore conveys the impression that formal compliance will be enough to legitimise their activities. It encourages a box-ticking mentality, rather than a more systemic, and systematic, approach to fulfilling its values. Data protection laws are written in accordance with this limiting framework, leaving official and other regulators, as well as the courts, with the task of filling in or applying more substantive considerations, sometimes drawn from Human Rights and other legal or philosophical precepts, such as proportionality, necessity, fairness, equality, and so on.

43.3. *Laws*

43.3.1. The global spread of legislative means to control personal-information processing has proceeded rapidly from the 1970s to the present time. Many countries have enacted sectoral and general laws for data protection, and most of these laws have established some form of specific enforcement and supervisory machinery. The latter, in the form of privacy commissioners and the like, are essential to the entire effort to safeguard privacy. The USA remains outside the 'club' of countries with comprehensive laws of this kind, thereby weakening global efforts to regulate surveillance, except in a piecemeal and patchy way. Sectoral and specific laws that control, for example, video surveillance, data-matching, censuses, or the use of genetic data, may have advantages in clarifying rights, but they also may override general proscriptions in favour of more pressing matters of public interest and policy, thus weakening protection. In some countries there are, in addition, common-law protections of confidentiality that have regulatory force over certain kinds of surveillance or invasive practices. The legal capstone, arguably, is human-rights legislation based on international declarations, and privacy commissioners have seen this as underpinning the legislation that they are charged with implementing. The efficacy of judicial remedies and of enforcement machinery such as regulatory agencies (e.g., privacy commissioners and 'supervisory authorities', in EU terms) varies according to the nature of cases, the statutory powers and sanctions available, the manner in which regulatory roles are performed, the resources provided by governments for this activity, and the range of issues and problems requiring an exercise of regulatory control.

43.3.2. None of these conditions give ground for optimism about the sufficiency of legal solutions, but their necessity seems in little doubt. They provide a countervailing set of limits to surveillance practices that may be challengeable on legal grounds – such as the disclosure to the CIA of customers' banking details in the SWIFT system of international financial transactions – and not only on grounds of outrage that is likely to prove ineffective by itself. That said, the weakness of many laws and their implementation machinery in the field of personal information processing has long been a matter for complaint, so that critics may have reason for impatience with legal solutions that may simply

[295] *op cit.* n. 281, ch. 1.

legitimate surveillance rather than regulate it.[296] Moreover, privacy and data protection laws do not easily regulate a wide range of surveillance practices, such as those that are part of modern telecommunications, and cannot easily be interpreted expansively to do so. There are also other laws, many of them passed in the interests of law enforcement and combating terrorism, that supersede or otherwise weaken the force of privacy laws; as discussed elsewhere in this Report, telecommunications data are particularly implicated in this. The role of courts and tribunals in determining the lawfulness of surveillant information practices has been crucial, although not necessarily always friendly to the cause of keeping surveillance and privacy invasion within tight limits. In addition, the harm that surveillance may do to individuals, groups and whole societies do not come within the range of impacts that these individual rights-based laws are designed to remedy or prevent.

43.4. *Self-regulation*

43.4.1. A variety of codes of conduct or practice have been developed by industries or companies, specialist bodies, and states, to regulate surveillance in many domains of activity, including CCTV, the activities of professionals, workplace monitoring, and so on. There are also online means of self-regulation by merchants who trade over the Internet, in the form of online privacy statements, 'seal' programmes and the like, backed up by organisations who vouch for them. Self-regulation is sometimes written into laws, as are codes of practice in the UK's Data Protection Act 1998 and in the EU's 1995 Data Protection Directive 95/46/EC. Increasingly, however, self-regulation is regarded as a better way of regulation given the 'failure' of laws and the less-regulated business climate that is considered desirable to foster.[297] Sometimes called 'soft law' or 'soft regulation', self-regulation prefers codes to legal rules and self-reporting to externally-imposed inspection. Yet it is hard to imagine the existence of codes and the like without the prior and parallel existence of laws or international instruments that are the sources of the very norms and guidelines that codes embody. The credibility and efficacy of self-regulation as a principal tool of surveillance limitation has not yet been generally demonstrated. It raises acute questions about accountability, supervision and transparency that foxes in charge of henhouses are unlikely to welcome, and that cannot be satisfactorily answered within the framework of self-regulation by itself. Comment elsewhere in this report about self-regulation in the telecommuncations field points out that there are many incentives for firms to ignore codes and the like; more generally, the sanctions that can be imposed by trade associations may not be severe enough to deter or punish their offending members.[298]

43.5. *Privacy-enhancing technologies*

43.5.1. Where once the critics of surveillance pursued a strongly anti-technology line of argument, a major development since the early 1990s has been the realisation that technologies themselves can provide powerful controls over surveillance or privacy invasion. This does not mean that 'technology is neutral', but that the surveillance or non-surveillance potentials of specific technologies depend upon how they are designed and deployed. Thus

[296] Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill NC: University of North Carolina Press.
[297] US Department of Commerce, National Telecommunications and Information Administration (NTIA) (1997) *Privacy and Self Regulation in the Information Age*. Washington DC: Department of Commerce, NTIA.
[298] *op cit*. n. 281, ch. 6.

encryption of personal data as it stored or flows across domains and other boundaries can range from the nonexistent to the very strong, network design and software 'code' can have a pronounced regulatory effect,[299] and web 'cookies' can be filtered in order to prevent profiling. However, there are great incentives for companies, governments and designers not to deploy 'privacy-enhancing technologies' (PETs) in their systems, or to make individuals pay or exert special effort to have them; or even to proscribe their use, as in the case of strong encryption. Surveillance, many would argue, cannot be reliably regulated through a 'technological fix'.

43.5.2. Some PETs are built into (or worse, bolted onto) ICT systems, whilst others are available to citizens and consumers, especially as they surf the net and engage in transactions, provided they have the knowledge, awareness and inclination to make use of them, and sometimes of the financial resources as well. Encryption, anonymous web-browsing, filtering devices, smart agents, privacy-preference tools and the like may act as empowering instruments for the individual. Whether, by themselves and as an alternative to other instruments, they are strong solutions to online surveillance practices is far from assured.

43.6. *Individual self-help*

43.6.1. This is a further broad category of regulation, in which the individual citizen or consumer controls her own information disclosure, possibly through the use of PETs, the exercise of choice in online transactions where opting-in or opting-out of certain information-processing procedures is offered, but also through knowledge, awareness and vigilance concerning the surveillance practices and privacy threats that befall her each day. All these put a premium on the individual's having sufficient interest in protection and the 'cultural capital' – the ability and the means to comprehend what is happening, to resist blandishments from information gatherers, to read obscure fine print on the web, and to assert herself in controlling inroads or seeking redress once these threats have been realised. In the USA, in the absence of regulatory or supervisory agencies, self-help, including initiating legal action, is the dominant means of privacy regulation, and criticisms of this model are legion. Other data-protection systems rely to some extent on individuals bringing complaints to the regulators and acting as frontline informants about dubious practices.

43.6.2. Property-based and market solutions are among the most prominent among self-help protections,[300] but have also been heavily criticised,[301] Market solutions mean that one pays, or pays extra, for one's privacy and one can sell one's information. Although solutions based on individuals' 'ownership' of their data could play a part in self-help, they may be limited in this role where the determination of ownership is not clear in information systems or in the use of certain technologies. However, although it is commonly argued that individuals should, and can, take responsibility for their own privacy and defence against surveillance, only a minority are probably able to exercise self-help as fully as 'responsibility' might imply, without a number of preconditions having been put in place to assist persons in their self-help or 'personal

[299] Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York NY: Basic Books.
[300] *ibid.*; Rule, J. and Hunter, L. (1999) 'Towards property rights in personal data', in Bennett, C. and R. Grant (eds.) *Visions of Privacy: Policy Choices for the Digital Age.* Toronto: University of Toronto Press; Laudon, K. (1996) 'Markets and privacy'. *Communications of the Association for Computing Machinery* 39: 92-104.
[301] Schwartz, P. (2000) 'Beyond Lessig's *Code* for internet privacy: Cyberspace filters, privacy control and fair information practices', *Wisconsin Law Review* 2000: 743-88; Rotenberg, M. (2001) 'Fair information practices and the architecture of privacy (what Larry doesn't get)', *Stanford Technology Law Review* http://stlr.stanford.edu/STLR/Articles/01_STLR_1

economy of protection'. Individuals may wish to be 'let alone', as one interpretation of 'privacy' would have it, but they cannot exercise controls 'on their own'.

43.6.3. These, then, have been the main categories of surveillance-limiting, privacy protecting instruments in use today. Further ones are being actively considered and promoted: Contracts and binding corporate rules for data transfers have also been prominent in the data-protection armoury. Other, less specific instruments, or rather, categories of persons playing important roles in the regulatory community, are significant as well, and may in fact be of crucial importance within each of these major types or overarching them in making general, society-wide contributions. We would here identify the activities of:

- privacy and anti-surveillance pressure groups, which – along with sections of the media – raise public awareness of issues and dangers, monitor situations, and exert pressure upon governments and businesses which make use of surveillance;
- technologists, who design surveillance and information systems, and whose education, training, and adherence to codes of practice may affect the awareness of their employers and shape the products;
- academic researchers, whose work may bring to light what is happening, explain why it is happening, and develop and test theories about the place and legitimacy of surveillance in the societies of the past, present and future; thus contributing expertise to public debate.

44. General Problems Concerning Instruments

44.1. Three of the most important problems with existing regulatory practices can be highlighted for discussion. The first two have to do with *fragmentation* and *weak co-ordination*. One problem concerns the main *instruments*; the other concerns the welter of jurisdictional *levels* at which regulation is supposed to take place. For both, the challenge is in terms of the potentially more unified and global surveillance challenge that regulation may be expected to face, giving the likely persistence of trends. For both, the question is how matters may be improved. In other words, can fire be fought with fire?: if the forces operating to extend surveillance are increasingly integrated and 'joined up', whether in any one country or internationally, how well integrated are the instruments and the levels of countervailing protective activity? The third problem is that of applying these instruments to the social effects of surveillance – and, perhaps especially, 'new surveillance' – beyond privacy invasion, or of fashioning new tools. For all three, there is room for rethinking the panoply of regulation in terms of how it can be made more coherent and effective. Full accomplishment of that task is beyond the scope of this Report, although some ground can be broken on identifying the issues. There is also room for considering the possibilities for privacy and surveillance impact assessment to be applied at whatever level and within whatever field, domain or sector of application. This, too, can only be indicated here.

44.2. Considering the instruments, those outlined above are usually considered as part of a 'toolkit' of regulatory mechanisms. But this metaphor fails to address the actual or desirable relationship of the 'tools' to each other, and how they can be better integrated. Indeed, it may be inappropriate to borrow the idea of 'tools' in the first place.[302] Most of the tools in a toolkit normally operate independently of each other,

[302] *op cit.* n.281, ch. 8.

and are specific to a particular purpose. On the other hand, the regulatory 'tools' are hardly independent, and are actually highly dependent upon each other if any of them is to work optimally at all. For example, international instruments depend upon national implementation and enactment. Laws depend upon the compliance of the regulated which, owing to the elusive and covert nature of many of the processes that are regulated, cannot be automatically assumed. Underpowered regulatory agencies need the media and pressure groups to put the spotlight on surveillance abuses, and need members of the public to bring complaints for investigation. They also need general political and administrative support from the governmental systems in which they operate, from their counterpart regulatory bodies in other jurisdictions, and from the business sectors that they both regulate and encourage to improve practices.

44.3. For their part, self-regulatory codes of practice may be more effective if laws and regulatory agencies require them or encourage them into existence in 'co-regulation' schemes, and may in turn require the willingness of participating organisations (e.g., firms in a trade association, or CCTV operatives) to adhere to them through staff training. Privacy-enhancing technologies may, or may not, be engineered depending upon the specifications of those – for example, governments – who procure the information and communication systems into which they may be designed. Technology designers rely upon market demand from industry and the public for their privacy-enhancing products, as the failures of many sophisticated anonymity and encryption tools has shown. Other illustrations of the 'toolbox' point about interdependency could be elaborated as well. The point is that the synergies and conflicts among the various instruments have not been adequately identified or recognised in practice, so that their potential as ways of regulating privacy invasions and the wider consequences of surveillance remains to be explored in depth. Moreover, it is not yet clear who, if any one, is to take responsibility for fostering the interdependent use of these instruments, or for designing their synergy in better ways.

44.4. Related to this last point, the second main problem, we argue, is that it is increasingly insufficient to consider that regulation takes place only, or mainly, at the level of each national (or other, whether smaller or larger) jurisdiction. The nation-state has been the main site of regulatory activity for some very good political, legal, economic, social and cultural reasons. The presence of international instruments and documents has been felt at the national level in terms of legislation, sometimes in implementation of international requirements, as in the case of EU Member States' transposition of EU Directives into national law. Sometimes, a foreign template or model for national legislative approaches has been adopted without such compulsion but where a country has experienced a 'ripple effect' and learned or borrowed from other countries,[303] or where solutions have been enjoined upon it by the actions of other countries or groups: the 'Safe Harbor' agreement between the USA and the EU is a case in point.

44.5. By and large, countries have not had to reinvent wheels; regulatory precedents and experience beyond national or jurisdictional boundaries have been a source for learning – or, indeed, for ignoring – worldwide. Be that as it may, regulation does, or may, take place at and across a series of levels or intersecting arenas from the local to the global and among different industries (e.g., telecommunications, marketing, transport, public services), taking into account the range of instruments. For example, and without comment on the effectiveness of the regulatory mechanisms involved, some workplace surveillance practices may be regulated at the level of the

[303] Bennett, C. (1997) 'Understanding ripple effects: The cross-national adoption of policy instruments for bureaucratic accountability'. *Governance* 10 (3): 213-33.

enterprise, where codes of practice may apply; but also at the level of the country in which it is located, if there are laws or overarching codes covering workplace activity; and at the global level, from which the International Labour Organization's code of practice on workers' privacy[304] originates.

44.6. Looking in another direction, the EU is not the only 'regional' or global arena that acts as a source or site of regulatory activity for some countries: the Asia-Pacific region has recently developed a Privacy Framework, albeit criticised as being of a low standard[305], and the World Trade Organization is another high-level arena with some potential regulatory force over certain global information flows and personal-data processing that have surveillance implications. The attempt to produce privacy standards to be followed worldwide has had a chequered and politically highly-charged career,[306] but nevertheless illustrates the way in which activity takes place beyond the borders of single nations, potentially affecting both them and the organisations that do business there, as well as their publics. Standardisation or privacy protection, beyond that for technical information-system security and including conformity assessment procedures for organisations, has been considered by many to be an important regulatory step, although so far its claims have not been strongly convincing in important policy arenas.

44.7. A further set of examples of international privacy-protection and surveillance-regulation activity at the regional level can be found within the EU and other European institutions. The EU's Article 29 Working Party, established under the Directive 95/46/EC and comprising Member States' commissioners, is noteworthy for the volume and range of its reports, opinions, working documents and the like, since 1997, on a host of topics that include the use of biometrics, video surveillance, the transfer of passenger name record (PNR) data from the EU to the USA, workplace surveillance, genetic data, RFID technology, and many more, totalling well over 100.[307] The establishment of the role of European Data Protection Supervisor (EDPS),[308] whose role includes monitoring ICT and other developments, advising on and influencing European Community policies in regard to personal data processing, and the evolution of global and lower-level networks, meetings and discussions amongst privacy commissioners on important topics and technologies, are among the ways in which activity relevant to regulation now transcends national boundaries. Other international or European bodies, such as Eurojust,[309] which assists in the investigation and prosecution of serious cross-border and organised crime, have their data protection officers and derivative rules for the protection of personal data.

44.8. However, estimates of the efficacy of these levels of work in preventing or remedying the more insidious forms of surveillance and privacy invasion can be debated, especially in the current adverse climate of opinion about the precedence that counter-terrorism and law enforcement must take over the values involved in privacy and the limitation of surveillance. There are also many gaps among official organisations in the development of roles, institutions, responsibilities and strategies for safeguarding against surveillance. Moreover, whether or not regulatory activities

[304] International Labour Organization (ILO) (1997) *Protection of Workers' Personal Data: An ILO Code of Practice.* Geneva: ILO.
[305] Greenleaf, G. (2005) 'APEC's Privacy Framework: a new low standard'. *Privacy Law & Policy Reporter* 11: 121-4.
[306] *op. cit.* n. 281, 105-8.
[307] See: CEC Directorate General Justice and Home Affairs (nd.) 'Art.29 Data Protection Working Party,' http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm .
[308] See: EDPS (nd.) 'Introduction,' http://www.edps.europa.eu/01_en_presentation.htm ; EDPS (nd.) 'Duties of the European Data Protection Supervisor and Deputy Supervisor,' ch.5.4, http://www.edps.europa.eu/01_en_sub_fonctions.htm#Chap_54
[309] See: Eurojust (nd.) http://www.eurojust.eu.int ; EDPS (nd.) 'Data Protection Officers appointed by the Community institutions and bodies,' http://www.edps.europa.eu/05_en_reseau_dpo.htm

among countries and across these levels can be co-ordinated, and agreed opinions used as the basis for effective influence in the governmental and world arenas in which authoritative policies and decisions are made, is also not certain. In the EU, national privacy-protection 'supervisory authorities' are enjoined to co-operate in certain activities, and there is an active set of European and global networks that share experiences and undertake investigations of specific topics and problems, so that regulators can become more knowledgeable, more effective and more co-ordinated. However, complicated political pressures and situations largely govern the fortunes of these and other forms of regulatory activity, although they do not nullify them.

44.9. The third main problem is that the regulation of surveillance, including privacy and data protection, has not kept pace with the advance of surveillance technologies, practices and purposes. Neither the data protection principles nor the fragmented condition of regulation machinery and instruments seem fully capable of meeting challenges that are likely to be posed in the future from public, private and combined sources. The advent of many new information and communication technologies (ICTs), including the Internet and mobile telematics, and the coming environment of AmI and ubiquitous computing that integrates many and varied surveillance devices, puts a question-mark over the efficacy of regulatory concepts and instruments that originated to handle issues in the age of the mainframe computer, or even of the laptop, the mobile telephone, and the Internet. There is also the question, raised in this Report's discussion of telecommunications in the United Kingdom, whether the overlaps between different national regulatory bodies, the confusion of responsibilities, and diverse interpretations of crucial concepts and terms, only adds to the difficulties or regulation. Moreover, the global nature of processes such as telecommunications makes the allocation of regulatory roles among national and international levels a pressing matter if uncertainty and weak control are to be overcome.

44.10. Regulatory issues and prospects arising in the world of RFID chips, devices for sensing, monitoring and tracking, biometrics and other technologies that will be increasingly used in workplace and domestic environments, and in travel and entertainment situations, are daunting. Online privacy,[310] once considered to be at the cutting-edge for privacy analysis, is not the end of the line for considering the possibilities of regulating the design and use of information technologies that process personal data. Online and AmI processes, moreover, interact, blurring the distinction between them, just as 'online and 'offline', 'manual' and 'computerised', 'public sector' and 'private sector' are no longer robust binary divisions for regulatory purposes. Codes of practice may be beside the point, and easily ignored, even if they could be devised. The old standbys of notice, choice, opt-out, opt-in, privacy preferences, privacy policy statements, privacy seals and the like may become tomorrow's irrelevancies in the world of information fluidity. Whether or not this proves to be true, how responsibilities should be distributed, and on whose shoulders they should fall, for improving consumer and citizen awareness and competence concerning risks, means of protection, rights and remedies are likely to remain important questions in the 'new surveillance' environment. So, too, will the question of how the privacy of the less easily educable and the technologically less capable can be protected; these, we should note, are not small and irrelevant minorities on the margin.

[310] Raab, C. (2006) 'The safe online consumer: Addressing issues and problems', Paper presented at the 56th Annual Conference of the International Communication Association, Dresden, 19-23 June, panel on *Individual and Social Perspectives of Online Safety*; Lace (ed.) (2005) *op cit.*, n.6.

44.11. These are not wholly new problems, in general: each generation of technology has seemed to make obsolete, in whole or part, the regulatory strategies that were devised for earlier ones. To some extent this has been anticipated, when, for example, laws eschew any mention of a specific technology, such as 'computers', so that they may remain relevant to technological change. But since at least the advent and spread of the Internet, the convergence of technologies and the interaction of online and offline information practices, the elasticity of regulatory regimes is sorely tested. If information collection and further processing, including transmission, is coming to be literally everywhere, both the capability of the instruments – even where they work in harness with each other – and of the jurisdictional levels and arenas – even if they were better integrated and rationalised – would be inadequate for many purposes, although still highly relevant to the control of the kinds of surveillance practices that are already familiar.

44.12. Moreover, insofar as the regulatory regimes that have evolved were designed mainly to control information privacy as conventionally understood, doubt also surrounds their ability to cope with the extension of surveillance in other domains where it is the body, the use of space, and other facets of privacy that are involved, as they are with many of the new technologies involved in the 'new surveillance'. The most coherent and elaborate repertoire of rules and techniques is concerned with the protection of personal information, rather than personal movement, physical presence in certain kinds of space, or bodily integrity as such, although these too are involved in the processing of information and personal data and to that extent remain governable by legacy regulatory systems. However, much ingenuity must be exercised in bringing the surveillance of these kinds of human behaviour under control by legal rules and understandings made for an earlier time, as many court cases attest. The alternative – creating new laws for each new technology or application – would only perpetuate the 'patchwork' nature of much privacy regulation, creating an ever-proliferating bewildering forest of special regulations that may go against the grain of pressures to simplify, unify and generalise controls. Data protection has already gone down the track of generalisation, with its comprehensive laws and multi-functional supervisory authorities, and has overcome the mind-set that once conceived of the private and public sectors as separate zones for regulation whilst the world, and flows of data, were working in the opposite direction. That said, certain sectoral laws and codes of practice are useful in conjunction with general approaches, and some of them are related to specific technological practices, such as telecommunications and video surveillance. Yet it is not easy to see how a family, such as the Joneses, would be able to employ a self-help repertoire against the ubiquitous and often surreptitious surveillance that occurs in their daily life.

44.13. These three sets of problems may not be the only ones to be identified, but they suffice to sum up many of the actual and potential shortcomings of regulation, identifying challenges that must be met if surveillance is to be kept under control and its adverse effects on a range of human values are to be mitigated.

45. Options for Future Regulation

45.1. *Privacy Impact Assessment*

45.1.1. We believe there may be considerable merit in adopting the approach of privacy impact assessment (PIA) in the regulatory practices of jurisdictions at

whatever level happens to be relevant.[311] PIA may best be seen as an instrument that those who propose new or revised information systems that process personal data can use themselves to mitigate the potentially harmful effects of these systems upon the privacy of the persons whose data are processed. Let us consider existing PIA theory and practice, whilst not overlooking its possible pitfalls and limitations.

45.1.2. In simplified terms, a PIA may be seen as:

- 'an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated';[312]
- 'a process. The fact of going through this process and examining the options will bring forth a host of alternatives which may not otherwise have been considered';[313]
- an approach and a philosophy that holds promise by instilling a more effective culture of understanding and practice within organisations that process personal data;
- a form of risk-assessment, which therefore cannot escape the uncertainties of identifying and estimating the severity and likelihood of the various risks that may appear, to privacy, life-chances, discrimination equality and so on;
- a tool for opening up the proposed technologies or applications to in-depth scrutiny, debate and precautionary action within the organisation(s) involved;
- like PETs, premised on the view that it is better to build safeguards in than to bolt them on;
- an early-warning technique for decision-makers and operators of systems that process personal information, enabling them to understand and resolve conflicts between their aims and practices, and the required protection of privacy above or the control of surveillance;
- ideally, a public document, leading to gains in transparency and in the elevation of public awareness of surveillance issues and dangers may be realised; in turn, it may assist regulatory bodies in carrying out their work effectively.

45.1.3. It is therefore not only the resulting PIA report that is beneficial, but the process itself. This technique is mandated in the USA and Canada for new federal-level public-sector projects involving the processing of personal data. Voices have occasionally been raised in the UK, calling for PIA to be applied to specific projects such as identity cards. The Performance and Innovation Unit[314] flirted with it in the context of data-sharing in the British public sector, and the National Consumer Council[315] recommended it for government and companies, calling for an amendment to the Data Protection Act 1998 to require it, and for the involvement of the Information Commissioner. A feasibility study was conducted in Scotland for the application of PIA to government's information-system plans for social care.[316] But there is resistance to developing and requiring an explicit assessment instrument in public organisations, even though government's profession to take privacy seriously in its long-standing ambitions

[311] Stewart, B. (1999) 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies,' *Privacy Law & Policy Reporter* 5 (8): 147-149; a descriptive discussion of PIA is given in Raab, C., 6, P., Birch, A. and Copping, M. (2004) *Information Sharing for Children at Risk: Impacts on Privacy*. Edinburgh: Scottish Executive.
[312] Stewart, B. (1996) 'Privacy impact assessments'. *Privacy Law & Policy Reporter* 3 (4): 61-4.
[313] Stewart, B. (1996) 'PIAs – an early warning system'. *Privacy Law & Policy Reporter* 3 (7): 134-8.
[314] Performance and Innovation Unit (PIU), Cabinet Office (2002) *Privacy and Data-Sharing: The Way Forward for Public Services*. London: Cabinet Office.
[315] Lace, S. (2005) 'The new personal information agenda', in Lace (ed.) *op cit.* n.6: 217-9.
[316] Raab, C. *et al., op cit.* n.310.

for e-government and IT-led public service implicitly incorporate something of the spirit, albeit not the letter, of PIA.

45.1.4. There are many and diverse models for implementation,[317] although they cannot be described here. The routines of applying a PIA require promoters of initiatives to understand, in detail, the flows of data in and around their systems, and to address issues beyond mere legal compliance, although some version of the inventory of principles, discussed above, is typically used as a basis. PIA should not be confused with compliance audits and the like, which are usually *ex post facto* and legally-oriented; as with environmental impact assessment, PIA assesses the likely impact of technology applications or new systems in the future, and considers a wider range of criteria. A growing practical literature has developed since the 1990s, largely related to the efforts of some privacy and data-protection regulators to develop and implement, or to encourage, the adoption of PIA as a precautionary instrument for assessing the likely impact upon privacy of new technologies or proposed information processing systems and practices.[318] One line of thought is that PIA could help to relieve the burden placed on regulatory officials to ensure the compliance, at the very least, of data controllers with laws and principles, and to deal with complaints from data subjects, by contributing to the design of technologies or practices is such a way as to reduce the adverse impact upon privacy.

45.1.5. Information systems and new ways of working in and across agencies are often put in place without a proper understanding of privacy requirements or other effects. Not having built safeguards into the processing of personal data, operators are then faced with having to add them, which is not always possible without expensive and embarrassing stratagems which may detract from the functionality of the system. For policy-makers at higher levels, PIA helps to ensure that the information systems established in the implementation of policies mitigate dangers (at least) or enhance benefits (at most). PIA assists the citizen in limiting the extent to which complaints and the search for remedies have subsequently to take place if a system or practice violates data protection or human rights requirements. PIA can therefore act to reassure citizens that the processing of their data, or other surveillance practices, are well protected or minimised; in so doing, PIA assists in the maintenance or creation of trust.

45.1.6. There is considerable political and administrative impetus towards surveillance, with privacy, confidentiality and human rights often seen more as an obstacle or as a restraint which, in the 'balance', should be accorded less weight. PIA may help to show how privacy protection can be accommodated within an information-sharing scheme as an important ethical and legal requirement that may contribute to important social and political objectives,

[317] A few examples are: Office of the Information and Privacy Commissioner of Alberta (2001) *Privacy Impact Assessment: Full Questionnaire*: Government of British Columbia Ministry of Management Services (2003) *Privacy Impact Assessment (PIA) Process.* Victoria: Government of British Columbia Ministry of Management Services; Ontario Information and Privacy Office (2001) *Privacy Impact Assessment – A User's Guide*. Toronto ON: Management Board Secretariat, Ontario Information and Privacy Office; Office of the Privacy Commissioner, New Zealand (2002) *Guidance Notes: Privacy Impact Assessment Handbook* Auckland: Office of the Privacy Commissioner, New Zealand; Treasury Board of Canada Secretariat (2002) *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks*, Version 2.0, August 31. Ottawa, ON: Treasury Board of Canada Secretariat; United States Department of the Interior, Office of the Chief Information Officer (2002) *Department of the Interior Privacy Impact Assessment and Guide*, Version: 9.16.02. Washington DC: United States Department of the Interior, Office of the Chief Information Officer.

[318] A useful general resource is Clarke, R. (nd.) *Privacy Impact Assessments* http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html . See also: Waters, N. (2001) 'Privacy impact assessment – traps for the unwary,' *Privacy Law & Policy Reporter* 7 (9): 176-7; White, F. (2001) 'The use of privacy impact assessments in Canada', *Privacy Files* 4: (7/8).

such as better, more citizen-oriented public service, or security, and not as an obstacle to them.

45.1.7. We can summarise and continue the discussion by itemising what PIA is *not*. It is:

- not a mere compliance tool: its proponents see it as a way of improving practice beyond the minimum necessary to conform to legal requirements;
- not an auditing mechanism: it assesses the impact of new and proposed systems, ideally before they are implemented;
- not, in most jurisdictions, a legally binding or definitive document: it may be influential or persuasive, and in some places (USA; Canada) the requirement to carry out a PIA is already a legal requirement;
- not imposed from outside: ideally, it is performed by, and 'owned', by stakeholders within an organisation;
- not a once-for-all process: it is subject to revision as systems or circumstances change;
- not a way of stopping the processing of data: it aims to facilitate it by analysing the privacy or surveillance risks and eliminating or mitigating them;
- not primarily a way of assessing risks to the *organisation*: the main aim is to reduce the risks to the data subject, although the organisation's risks are also considered;
- not a universal template: although there are exemplars; the PIA should be tailored to assess the information processes of the particular organisation;
- not a tick-box exercise giving an answer or 'score' at the end: it is a way of raising questions that need to be answered and highlighting issues that need to be resolved.

45.1.8. It is also not a 'magic bullet' capable of being incorporated into business or state operations without financial costs and changes in working practices, although the avoidance of expensive mistakes and the political, reputational and trustworthiness gains should be set against these outlays. It may not be easy to undertake a PIA, nor does it promise an easy 'fix' for the dilemmas involved in decisions about implementing surveillance. Common failings are a perfunctory, compliance-oriented and box-ticking approach to investigating effects; a feeling of alienation from the process, particularly if the PIA is not led and championed from within the organisations concerned; and a disconnection between the PIA process, its results, and crucial decisions. Ideally, a PIA tells the story of an information system or technological application: 'why it exists and how it collects, uses, discloses, and retains personal information. In this process, specific privacy issues are surfaced and can be resolved in a comprehensive manner on the basis of clear thinking and accurate information'.[319]

45.1.9. On the other hand, it may be difficult to ascertain all the required facts about a system, and the risk-assessment that lies at the heart of PIA cannot be straightforward. Risks may be difficult or impossible to quantify, although the PIA discipline presses those involved to explore, discuss and perhaps debate the question of risk publicly, rather than simply assuming conventional understandings. PIA thus promotes reasoned approaches to the relationship

[319] Flaherty, D. (2004) 'Privacy impact assessments (PIAs): An essential tool for data protection'. Paper presented at the Privacy Laws & Business 17th Annual Conference, Cambridge, 5-7 July, 2.

between privacy and other, sometimes competing, priorities. In so doing, it may strengthen transparency and accountability. PIA should not be a once-for-all exercise: the result should be capable of updating as systems change, as they inevitably do. When one is considering a PIA approach to joined-up, inter-organisational working and information-sharing, the difficulties may be multiplied. However, the systematic questioning that PIA involves may be a strategic point of entry into a host of issues concerning information custodianship, leadership, roles, protocols, and so on, which are already considered essential to good organisational, and inter-organisational, practice.

45.2. *From Privacy Impact Assessment to Surveillance Impact Assessment?*

45.2.1. To encompass the potentially harmful effects of surveillance on a wider basis than that of protecting privacy, it would be necessary to develop PIA tools beyond their existing configuration, and to develop what could be called *surveillance impact assessment*, or SIA. This, of course, involves a change of meaning, for whereas PIA assesses impacts *of information processing on privacy*, SIA would assess the impacts *of surveillance on a range of values* that may include, but also transcend, privacy itself.

45.2.2. An important drawback, but also an opportunity for further development, has to be recognised. Here we return to our earlier remarks about privacy protection and its relation to surveillance protection. Because PIA has been innovated as a tool for looking at *privacy*, conceived in terms of individual rights, it is not at present best suited to embrace the further ramifications of surveillance in terms of a range of other social and personal impacts. Doing this would require something of a paradigm shift from considering only the effect on *individuals*, as privacy policy tends to do, to considering the value of privacy protection and surveillance limitation in *societal* terms as well.[320] Privacy is not only an individual value, but is also important for society as a foundation for the common good and for values held in common, such as democracy, trust, sociability, and a free and equal society. This is occasionally, but not certainly, reflected in the approaches taken by official privacy regulators, enlightened companies, and privacy advocates. Because the value of privacy extends beyond the individual, we all have a stake in the right, and the ability, of any individual to have her privacy protected by whatever instruments. Both privacy itself, and privacy protection, are socially valuable, embracing common, public and collective dimensions. Albeit an individual value and a human right, privacy is also a common value because all persons have a common interest in a right to privacy even though they may differ on the specific content of their privacy or what they regard as sensitive. It is a public value in that it is a sustaining principle of a democratic society. It is a collective value insofar as it is – in some respects and with some regulatory instruments – a collective good that cannot be divided, from the protection of which individuals cannot be excluded, and which cannot be efficiently provided by the market. [321]

45.2.3. If this is so of privacy, it is emphatically so of surveillance and its regulation, because many surveillance practices have a direct effect on the nature of the society in which they are embedded, in terms of categorical discrimination (or empowerment), social exclusion, and other outcomes that would still be causes of concern even if the invasion of individual privacy were not in question. PIA, and privacy regulation as a whole, would benefit from

[320] Regan (1995) *op cit.* n.14, ch. 8.
[321] *ibid.*

taking on board the social value of privacy. Nevertheless, taking social effects into consideration would be a sea-change in the world of privacy protection, its instruments and its regimes. There may not be many national or other jurisdictions' privacy regimes that would regard it as legally or politically possible to expand their horizons, and specifically the roles of regulatory participants, to embrace these broader effects, which are more palpable when considered in the idiom of surveillance. The regulation of surveillance has as its main objective the safeguarding trans-individual, social values, in addition to individual privacy values. This is why SIA could play a valuable role by incorporating PIA but transcending it with a range of enquiries aimed at assessing the impact of surveillance, or privacy invasion, upon society itself and upon the other, non-privacy, interests of separate individuals, categories and groups.

45.2.4. There are precedents for expanding the horizons in other fields: environmental impact assessment has become embedded in governance arrangements that previously only had, say, food-production, transport, energy supply, industrial or housing development as their remit and responsibility. The impact of government policies upon ethnic or racial minorities is now also recognised as something that needs to be taken into account. What an ICT innovation, a new database, or a new audio-visual scheme for monitoring public places or private shopping precincts, implies for personal autonomy and dignity, social solidarity, or the texture of social interactions, is not an inconceivable line of enquiry that could become institutionalised as a set of practices and requirements before those surveillance possibilities are implemented.

45.2.5. We made mention, earlier, of Marx's questions concerning the ethics of surveillance: these could lend themselves to SIA as a development of PIA, and we append them to this section of the Report. Adapting questions such as these to assess surveillance's impact takes the enquiry into realms of where the means, the data collection context, and the uses of surveillance are assessed for their impact upon individuals and communities in terms of physical or psychological harm, inequitable distributions of processes, power imbalances, and many others, including standard data-protection compliance criteria of awareness, consent, redress, sanctions, purposes, and so on. This repertoire is rooted in a mainstream ethical stance, but also in a certain legal framework that has already been established through the international instruments and laws that we have already seen, so that wholly new foundations need not be laid for something like this type of enquiry to inform SIA, and indeed PIA. Whether new *political* foundations would need to be laid is a question to be addressed in states and other entities, and is not for this Report.

45.2.6. We cannot demonstrate at length, in this Report, how SIA would be applied in practice, but some of Marx's questions can be highlighted as the kinds of question that an SIA would ask, apart from those questions – the majority – that are more directly related to privacy as such. For example, enquiring about harm ('does the technique cause unwarranted physical or psychological harm' or 'disadvantage'?) taps into the implications for personal well-being that may not necessarily be remediable under data protection laws, or addressed by other laws that protect privacy. Enquiring about the beneficiaries ('does application of the tactic serve broad community goals, the goals of the object of surveillance, or the personal goals of the data collector?') is not designed to discredit the latter two, but to gain a purchase on the implications of the surveillance technique so that the enquirer knows where the investigation should go next. Enquiring about the consequences of inaction

('where the means are very costly, what are the consequences of taking no surveillance action'?) is aimed at assessing the necessity of the surveillance, not merely its feasibility and desirability.

45.2.7. These are only some illustrations of the line of investigation that an SIA could take, and it is obvious that it would range more widely than questions about legal compliance or even about personal privacy. Any SIA, like any PIA, would have to be tailored to the specific characteristics of the practices or technologies in question,[322] although there would be a broad, basic similarity among investigations across an array of practices, because they have much in common and because there are common legal or ethical requirements that they would have to meet.

45.2.8. As mentioned earlier with regard to PIA, one advantage that SIA could have is in assisting regulatory agencies and individual citizens to understand and control surveillance practices by making them more transparent and their proponents more accountable. These, in fact, are among the principal aims of freedom of information (FOI), which forms part of the enforcement responsibilities of a number of privacy regulatory bodies or of commissioners established specially for that purpose. If SIAs were required of firms or public organisations and made public as the basis of further discussion as well as approval, they would play a part in opening up surveillance to public scrutiny and comment. Moreover, as many have argued with regard to PIAs, there are benefits to the organisation's understanding of its own practices and how they can be improved in order to make them more compliant with the law, with codes of practice limiting surveillance, and/or with the image of integrity and trustworthiness that the organisation is trying to project.

45.3. *Other Options*

45.3.1. If SIA builds upon PIA, other options also build upon the present. We have in mind, especially, how privacy commissioners and other regulators can expand their role – if their political systems will make it possible to do so – to embrace the regulation of surveillance more widely conceived. There are no recipes for overcoming many of the difficulties that privacy commissioners have experienced, in many countries, in exercising their authority under existing legislative enactments at whatever jurisdictional level, and between them. Moreover, there are specific problems with the exercise of these regulatory roles that may not have been experienced everywhere.

45.3.2. In the face of the 'new surveillance' but also with regard to conventional challenges, we think it would be in order for regulators to have more powers and resources, more sanctions available to them for use, greater influence over government policy and business plans, less burdensome routine requirements, and greater public visibility. This is likely to be read as a wish-list to which few members of the regulatory community would object, but it would be unrealistic for this Report to put forward more specific recommendations of this kind as a shopping list addressed to no-one in particular, or pertinent to no situation in particular. That said, it is possible to enumerate some particular improvements that seem desirable and also, in many cases, feasible; or at least to indicate where a reconsideration of the regulatory environment and process might be in

[322] A brief discussion, in the context of AmI, is in Raab, C. (2006) 'Regulating ambient intelligence: The road to privacy impact assessment?' Paper presented at the International Conference on Safeguards in a World of Ambient Intelligence (SWAMI), Brussels, 21-22 March.

order. These relate to the six areas of difficulty that were identified at the beginning of Part D:

- Reactive regulation: official regulators have often been taken unawares by business or governmental ICT or systems proposals that pose potential threats to privacy or that have ominous surveillance capabilities. Regulators, whether official or civil-society members of the privacy and surveillance policy community, may be sidelined from the policy and decision arenas in which these plans are developed and implemented, or may enter them too late to have influence upon them. PIA or SIA may help in fostering a more proactive regulatory approach, but only to the extent that access to policies and plans occurs early enough. As far as regulatory agencies are concerned, it would be helpful if their early intervention and scrutiny were supported by statute or other binding requirement. But the ability to enter the arena is, in many cases, only as good as the regulators' ability to keep abreast of, and knowledgeable about, new technologies and systems; for this, their institutional capabilities may need improvement, which would have resource consequences. These may be difficult to be borne at the level of each jurisdiction. Therefore, it is advantageous further to develop a pooled technological knowledge-and-awareness capability, as may be occurring, for instance, at the level of the EU, through the Article 29 Working Party and other networks and channels in which many national and sub-national regulators participate.

- Technical and managerial regulation: an antidote to the procedural emphasis of much regulation, mentioned as the second area of difficulty, would be partially found in these strategies and instruments. They would assist anticipation as well as, in the case of PIA and SIA, help surveillance proposers to mitigate undesirable effects through organisational change, staff training, privacy-friendly information-management improvements, and so on. This would help to put law-based regulatory approaches into a wider context of strategy; this may already be present in many regimes, although probably less so at the international level, but needs to be underpinned. It would also be helpful if the movement to develop privacy standards at the international level were to gain impetus; standardisation would simplify the regulatory burden placed upon official agencies and would assist in organisations' efforts at self-regulation, as well as providing a measure of public assurance. This might be especially useful in the context of new technologies and information processing that is based on them. It would also demonstrate useful synergy between some of the regulatory instruments described earlier.

- The conception of 'privacy': we have already remarked on this, explaining the need for a wider view of, broadly speaking, the social value of privacy as it is implicated in safeguarding privacy and limiting surveillance. The notion of the 'public interest' is also implicated in these conceptual problems, especially where privacy and the public interest are placed in adversarial positions by the way political and regulatory discourse, not to mention public debate, is constructed. Serious reconsideration of these concepts, and of their relationship in specific contexts, could help to underpin the way in which privacy principles are invoked and also extended to cover novel situations presented by the

'new surveillance'. Otherwise, privacy and the limitation of surveillance is highly likely to be the loser in any 'contest'.

- Public debate: the level of public debate about privacy and surveillance is very low in general, and, with exceptions in some countries or at some times, disconnected from current government policy proposals or commercial innovations. There seems to be a 'Serious' debate and public debate are largely separate worlds, although there are many weblogs in which important debate is carried on and engaged with current proposals. It would be useful to undertake an assessment of the existing role of the conventional and 'new' media, of civic organisations and professional associations, of academia, and of other organs of debate and communication, in encouraging public knowledge, awareness and debate beyond the often tendentious approaches of business, governmental interests and pressure groups to sway public opinion in one direction or another. Improvements might follow such an assessment; but a danger in implementing these might be a tendency to patronise and 'enlighten' the general public, which, in the case of the 'public understanding of science' has often had deleterious results.

- The burden of regulation: there are, indeed, costs of privacy and surveillance regulation and costs of compliance. There needs to be an independent assessment of what these are and who bears them, and a judgement made, on the basis of explicit and agreed criteria, of whether these costs are 'excessive', whether they 'outweigh the benefits', whether they actually do 'inhibit initiative, risk-taking and productivity', as is often claimed. On the other side of the coin, the benefits of regulation need similar rigorous analysis. It can be said that the gains in public trust and organisational efficiency that may come from good privacy protection and surveillance regulation are only recognised to a limited extent; but they, too, require impartial analysis. However, the economics – or political economy, for it is not just an 'economic' question, but one of political and social values more generally – of privacy and surveillance is an underdeveloped speciality, and there is probably no off-the-shelf model that can be adopted without serious adaptation. If that is so, it is perforce so of what is often seen as the third step: 'balancing' the costs with the benefits. We are far from persuaded that the ambiguous doctrine of 'balance', which pervades privacy protection practice and rhetoric, can stand up to serious scrutiny, but it should be exposed to it.[323]

- Media discussion: the mass media's treatment of privacy and surveillance issues tends to be dominated by clichés, an oversimplified 'contest' mentality, the latest 'horror story' about how the failure of organisations to exploit personal data has led to tragic deaths, or (conversely) how 'they' are surreptitiously building large databases, and the like. As mentioned above, taking stock of the role of the media is in order, as is the consideration of what role it is able to play in future. Complex ethical and social issues, as well as technological developments, are very difficult to discuss in the press, broadcasting, and in other media, and, in any case, 'the public' as well as 'the media' are segmented and highly varied. These pose formidable tests for any attempt to elevate the tone of the media.

[323] Raab, C. (1999) 'From balancing to steering: New directions for data protection', in Bennett and Grant (eds.) (1999), *op cit.* n. 299.

45.3.3. Finally, something should be said about the way regulation could be improved through a consideration of how adequate the relationships, and the interdependence of tasks, are between regulatory systems at different levels up to the global, and between different kinds of participant, including regulatory agencies and groups in civil society. We have hinted at this question with regard to telecommunications. It is difficult to say much about this matter in the abstract, but it remains for further discussion how far, for example, the co-operative relationships that were indicated in the EU Directive 95/46/EC have served not only enforcement and compliance purposes, but intelligence-gathering and issue-awareness on the broader front of surveillance practices and technologies. Or, for another example, how far there is a mutually productive relationships between regulatory agencies and civil-society groups that both assist these agencies when the latter draw issues and useful information or knowledge to their attention, and act as a gadfly when regulation appears to falter or when government and business practices seem to extend surveillance. Whether there is room for further innovation of independent roles in the regulatory system, apart from committed regulators and committed anti-surveillance advocates, is another matter for exploration beyond this Report, which perhaps serves as one kind of illustration.