A Report on the Surveillance Society

For the Information Commissioner

For the Information Commissioner, by the Surveillance Studies Network

Summary Report

September 2006

Edited by:

Kirstie Ball and David Murakami Wood

From material by:

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

Introduction

In June 2006 the Surveillance Studies Network was commissioned, by the United Kingdom Information Commissioner, to write a report on the surveillance society. This document is a summary of that report. It is split into three sections which cover the essential material in the report. The first maps the terrain of the surveillance society: its definitions, issues and consequences. The second shows how the surveillance society operates. The third examines some of the regulatory challenges posed by the surveillance society.

1. Surveillance Society: summary, history, definitions

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. It is not just that CCTV may capture our image several hundred times a day or that check-out clerks want to see our loyalty cards in the supermarket. It is that these systems represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living.

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, called 'bureaucracies'. 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. Impersonal and rule-centred practices spawned surveillance. New, post war, information technologies revolutionized bureaucratic administration, enhancing speed, control and co-ordination. This, coupled with improved identification and tracking techniques developed in military and police departments, constitutes the main message of this report. Surveillance grows as part of being modern.

What's wrong with surveillance society?

Understanding surveillance society as a product of modernity helps us avoid two 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 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.

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. Large-scale technological infrastructures are prone to large-scale problems. 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.[1]

It is equally important to consider corruption and skewed visions of power. Again, we do not have to imagine some wicked tyrant getting access keys to social security or medical

[1] 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/

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. 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.[2]

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 Experian. 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.[3]

Most profoundly, all of today's surveillance processes and practices bespeak a world where we know we're not really trusted. Surveillance fosters suspicion.[4] 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.

Defining surveillance; tracing surveillance society

The surveillance society is a society which is organised and structured using surveillance-based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure our society. This information is then sorted, sifted and categorised, and used as a basis for decisions which affect our life chances. Such decisions concern our entitlement and access to benefits, work, products and services and criminal justice; our health and well-being and our movement through public and private spaces. Everyday encounters with surveillance include:

- Video cameras which watch us everywhere we go – in buildings, shopping streets, roads and residential areas. Automatic systems can now recognise number plates (and increasingly faces).
- Electronic tags which make sure those on probation do not break their release conditions, and people arrested by police have samples of their DNA taken and kept whether they are guilty or not. 'Criminal tendencies' are identified earlier and earlier in life.
- We are constantly asked to prove our identity, for benefits, healthcare, and so on. The UK government now plans to introduce a new system of biometric ID cards, including 'biometrics' (fingerprints and iris scans) linked to a massive database of personal information.

[2] 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

[3] 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.

[4] This is discussed in: Lyon, D. (2003) *Surveillance after September 11*, Cambridge UK: Polity Press, 45-48, 142ff.

- When we travel abroad, who we are, where we go and what we carry with us is checked and monitored and the details stored. Our passports are changing: computer chips carry information, and like ID cards, there are proposals for biometric passports.
- Many schools use smart cards and even biometrics to monitor where children are, what they eat or the books they borrow from the library.
- Our spending habits are analysed by software, and the data sold to all kinds of businesses. When we call service centres or apply for loans, insurance or mortgages, how quickly we are served and what we are offered depends on what we spend, where we live and who we are.
- Our telephones, e-mails and internet use can be tapped and screened for key words and phrases by British and American intelligence services.
- Our work is more and more closely monitored for performance and productivity, and even our attitudes and lifestyle outside work are increasingly scrutinised by the organisations that employ us.

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. To break this down:

- The attention is *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 everyday business.
- Surveillance is also *systematic*; it is carried out according to a schedule that is rational, not merely random.
- Lastly, it is *focused*. Much surveillance refers to identifiable persons, whose data are collected, stored, transmitted, retrieved, compared, mined and traded.

The personal details in question may be of many kinds, including CCTV images, biometrics (fingerprints or iris scans) communication records and content, 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.'[5] 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

Perspectives on the Surveillance Society 1: Processes

We turn now to an inventory of processes and issues 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.

Social sorting is endemic in the surveillance society. In government and commerce large personal information databases are analysed and categorized to define target markets and risky populations.[6] Once classified, it is difficult to break out of the box. 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. Social sorting increasingly defines surveillance

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

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

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.

Data flow: 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. That logic needs to be questioned, examined and checked, particularly in regard to processes that involve data-flow from one setting to another.

Function Creep occurs when personal data, collected and used for one purpose and to fulfil one function, migrate to other ones that intensify surveillance and privacy invasions 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.[7] Function creep usually happens quietly, as a bit of administrative convenience. Indeed, because new technologies permit increasing amounts of data interchange and because organizational efficiency is frequently seen as a top priority, the human consequences of function creep are all-too-often unknown, ignored or downplayed.

Technologies: Technologies are critical to surveillance, but two important things must also be remembered: One, 'human surveillance' of a direct kind, unmediated by technology, still occurs and is often yoked with more technological kinds. Two, technological systems themselves are neither the cause nor the sum of what surveillance is today. We cannot simply read surveillance consequences off the capacities of each new system. For the surveillance society properly to be understood, we have to understand how technologies work, 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.

A further 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 (PETs) serve well to curb the growth of technological surveillance 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 too complex for such superficial responses.

Perspectives on the Surveillance Society 2: Issues

*Privacy, ethics, human rights***:** 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)[8] have evolved it has proved difficult to persuade policy-makers of the salience of the *social* dimensions of privacy[9] let alone of the need to confront problems associated with the surveillance society as such. Surveillance society poses ethical and human

[7] 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

[8] FIPs are the North American equivalent of European 'data protection principles.'

[9] 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.

rights dilemmas that transcend the realm of privacy. Ordinary subjects of surveillance, however knowledgeable, should not be merely expected to have to protect themselves. Three key issues are as follows:

Social exclusion, discrimination: 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. 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.[10]

Choice, power and empowerment: 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. 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.[11] 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. Individuals are seriously at a disadvantage in controlling the effects of surveillance.

Transparency, accountability: Individuals and groups find it difficult to discover what happens to their personal information, who handles it, when and for what purpose. Yet little by little, their personal data are used to help shape their life chances, to guide their choices. Given the power of large organisations with sophisticated surveillance capacities, however, it seems only fair that ordinary people should have a say, even if only at the level of principle. This may be sought, not only through specialized agencies but also through advocacy groups and the mass media.

Accountability should be assumed within organisations, especially when high-powered surveillance occurs routinely, with potentially damaging consequences. Although workplace surveillance offers some salutary examples of poor practices at least in some instances employers have been obliged to curb the excesses of their monitoring by active labour union intervention. And much can be achieved through a transparent process of employers explaining what monitoring entails and obtaining negotiated consent 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.

2. A Survey of the Surveillance Society

The Surveillance Studies Network commissioned a number of expert reports which 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

[10] Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
[11] See the *New York Times* editorial, 'The data-fleecing of America' June 21, 2005.

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.

The Context of the Surveillance Society

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

Risk and Security: We live in a society obsessed by risk. Risk management techniques dealing with external and internal threats have become a key part of organisational activities. A *pre-emptive* as opposed to a *preventative* approach to risk has emerged.[12] Significantly, use of data-mining and profiling to identify risks shifts surveillance practices toward the screening of the actions and transactions of the general population.[13] 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. Collection and analysis of information, including data on identifiable individuals are vital. 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

Several examples illustrate this trend to risk assessment and pre-emption:

- Epidemiology and modelling within medical surveillance,[14] to identify individual cases, record occurrences for statistical analysis and identify categories of the population who are at risk for particular diseases
- Risk assessment of individuals, families and neighbourhoods in child protection, mental health and criminal justice
- Categorising the risk travellers pose to national security using passenger manifests and financial transactions
- Evaluating the relative value of individual consumers, and their geodemographic profiles

The Militarization of Surveillance: Military surveillance is one of the few phenomena that can be said to be truly global in an age where everything is supposedly being globalised. The Earth is surrounded by a multitude of military surveillance satellites and transnational communications systems are thoroughly infiltrated by military surveillance systems. With the Global Positioning System and the Internet as two contemporary examples of technologies designed with military capability built-in, 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 totally defensible and secure space[15]. 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. ‘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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

penetration and security specialists are redesignated as 'knowledge warriors'. Many surveillance technology companies are intimately bound up with the military yet sell to civilian users too. For example TRW, a major partner of the US defence contractor became a leader in civilian biometrics; French company Sagem manufactures everything from mobile phones through surveillance algorithms to unmanned aerial reconnaissance systems.

The Political Economy of Surveillance: 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. The security industry has grown massively in recent years. According to the US consultancy Security Stock Watch's 100 company index[16] the growth of the industry as a whole has consistently outperformed both the Dow Jones and the high-technology NASDAQ indices[17]. 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.

Personal Information Economies: Surveillance is not just conducted by states and organisations but also by ordinary people. After the 2005 London bombings, 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[18] and social networking sites like *MySpace* and *Bebo*. At the same time, those with greater access to knowledge resources are starting to manage their 'data double' found, for example, in the databases of credit referencing agencies such as *Experian* or *Equifax*. These agencies allow individuals online access to their credit- records, enabling them 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.

Surveillance Technologies

Whilst it is vital not to forget the importance of non-technological surveillance (for example, eavesdropping, spying and surveillance involving direct human judgement), this section will focus on issues connected with surveillance technologies. We will first concentrate on overlapping advances in four areas: telecommunications; video surveillance; databases; biometrics and location, tagging and tracking technologies. We will then consider interconnections between different technologies and the trend for surveillance technology simultaneously to vanish and spread everywhere. We will conclude by considering the limits of technological development.

Technological Development: It is indisputable that new technologies have helped to change the nature of surveillance. There is no inherent 'good' or 'evil' within these technological systems. Efficient national databases can be used for the provision of targeted health care or for the victimisation of political opponents. But it is also not a simple matter of how they are used either. All technologies are developed within particular organisations which have particular aims and interests. Several particular technologies and their capabilities will be examined

Telecommunications: Surveillance in telecommunications refers to the degree to which individuals, organisations and corporate bodies are able to monitor, sort and store information

[16] This index includes 'biodefense', 'environmental security', 'fraud prevention', 'military defense', telecommunications network security' and 'physical security' (barriers, video surveillance etc.) industries.

[17] *SecurityStockWatch.com 100 Index*, August 2006, http://www.securitystockwatch.com/

[18] 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

about the occurrence and content of telecommunications exchange, both between technological devices, and between technological devices and people. Since the state began 'wiretapping', technological development has led to more diverse technologies employed for telecommunications, and greater surveillance capability. 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. 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, 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[19].

Video Surveillance: Photographic surveillance has been in existence since the late 19th century. 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,[20] and a person can be captured on over three hundred cameras each day.[21] During the 1990s the Home Office spent 78% of it crime prevention budget on installing CCTV[22] and an estimated £500M of public money has been invested in the CCTV infrastructure over the last decade.[23] However a Home Office study concluded that 'the CCTV schemes that have been assessed had little overall effect on crime levels'.[24] Digitisation has allowed the automated use of CCTV systems to grow. 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.[25] This increase in state surveillance has received a consistently negative press,[26] despite the fact that speed cameras, unlike open street CCTV have a significant impact in reducing death and injuries cause by traffic accidents.[27] There are plans to expand capity at the National Automatic Number Place Recognition (ANPR) centre from 35 million reads per day to 50 million by 2008.

The 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. Surveillance which uses databases can be usefully thought of as 'dataveillance.' 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. Dataveillance is seen extensively in marketing, medicine, policing and border control.

[19] 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.

[20] McCahill, M. and Norris, C. (2003), 'Estimating the extent, sophistication and legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press.

[21] Norris, C and Armstrong, G. (1999), The Maximum Surveillance Society: The Rise of Closed Circuit Television, Oxford: Berg.:42

[22] *ibid.*: 54

[23] 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.

[24] Gill, M. and Spriggs, A. (2005). *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate, 43, 60-61.

[25] 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.

[26] McCahill and Norris, 2003 *op cit.* n.44.

[27] 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

For example, in *marketing* as the cost of databases has decreased, many private sector corporations seek to gather as much data on their customers as possible and target their marketing more specifically. Transactional data (use of credit cards, mobile phone calls etc) traceable to a person are combined with additional data from loyalty card programmes, customer surveys, focus groups, promotional contests, 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. These are most readily connected to postal codes, and given streets are 'profiled' with terms like 'prudent pensioners', 'fledgling nurseries' to 'rustbelt resilience.'[28] 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.[29] 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.[30]

Biometrics: All new ID systems 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 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. The 'War on Terror' has produced a surge in research funding for and the implementation of biometrics. 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.[31] 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. In the UK, the aforementioned shift towards digital CCTV has led to further research into the practicalities of biometric CCTV systems and facial recognition, following early experiments in Newham, Birmingham and other locations.

Locating, Tracking and Tagging: Surveillance practices are increasingly referenced, organised and located through Geographical Information Systems (GISs)[32]. Many 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. Some current applications of these technologies are in law enforcement, border management and the workplace:

[28] 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*.

[29] 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.

[30] 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.

[31] 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.3.

[32] Institute for the Future (2004) *Infrastructure for the New Geography,* Menlo Park, CA: IFTF.

For example, in *law enforcement*, in 2004/5 some 631 adults and 5751 juveniles, some as young as twelve years old, were 'tagged' allowing them to await trial at home rather than be remanded into custody.[33] Offenders released from prison are also subject to electronic monitoring either as a condition of early release from prison under the Home Detention Curfew Scheme[34] or as a condition of being released on Parole.[35] In US *border management* RFID-enabled border smart cards are being trialled at the US-Mexico border. 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. Starting with animals, living beings are beginning to be implanted with RFID. In the US 70 people with degenerative brain conditions have also been implanted so they are more easily tracked[36], and one company chipped two of its employees for *workplace* access control. [37]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.'

Technological Synergy and Function Creep: 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. For example:

- IDs that work for several purposes – border crossing, fraud control, access to government information and perhaps commercial (video rental) and semi-commercial (libraries) too. 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 does seem somewhat undermined.
- ANPR in London 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.

Towards Pervasive Surveillance: Technologies are at their most important when they become ubiquitous, taken for granted, and largely invisible. Pervasive or ubiquitous computing (Ubicomp), also known as 'ambient intelligence' (AmI), creates the conditions for pervasive or ubiquitous surveillance by being simultaneously embedded in the physical and virtual environment.[38] Electronic services and realms are relatively easy to control compared to physical urban streets, but many urban 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

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

[34] 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).

[35] NPS *op cit.*

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

[37] 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 .

[38] Kang, R. and Cuff, D. (2005) 'Pervasive Computing: Embedding the Public Sphere,' *Washington and Lee Law Review* 62(1): 93-146. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57: 43-49.

track movements and behaviours of millions of people in both time and space. In industry parlance, this is called multiscale spatiotemporal tracking.[39]

The Limits of Technology: 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. There are also concerns about reliability,[40] '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.[41] Similar problems with law enforcement technologies such as facial recognition and ANPR have also been identified

Technological Lock-in and Regulatory Lag: Surveillance technologies frequently get promoted unproblematically as 'the answer' to multiple threats, most recently to the threat of terrorism. However the more that we 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. Regulators are constantly running behind technological innovation, unable to understand 'how it works'. In this constant chase, one has to ask whether states possess the necessary tools to carry out meaningful regulation of complex surveillance 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.

Surveillance Processes

The importance of pre-emptive risk assessment, and the prescription of surveillance as a solution to all kinds of problems has given rise to a number of processes and phenomena unique to it. Social sorting, unforeseen consequences, information sharing and a blurring of the public and private are four examples.

Social Sorting, Categorisation and Targeting. Social sorting, the sorting of the population into different categories of risk, entitlement or value, can be observed in many areas:

- Consumers continually supply businesses with their transaction data, and are part of an evolving feedback loop that binds acts of consumption with the gathering of data and the generation of profiles.[42] Call centres now rank order customer accounts according to their relative spend, and alter their service levels accordingly. The Telecoms industry records traffic data to identify the best routes to market (e.g. marketing by SMS)
- Call centre employees are assessed for social and lifestyle factors which match those of the market segment they are serving.
- 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.

[39] Hampapur, A. *et al.* (2005), 'Smart video surveillance', *IEEE Signal Processing Magazine*, March: 38-51.

[40] See: Zureik, E. with Hindle, K. (2004) 'Governance, security and technology: the case of biometrics' *Studies in Political Economy*, 73: 113-137.

[41] See: Grayling, A.C. (2005) *In Freedom's Name: The Case Against Identity Cards*, London: Liberty.

[42] Detailed in: Elmer, G. (2004). *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA: The MIT Press.

Unintentional Control: Surveillance should not be taken to be identical with direct social control.[43] The intention of surveillance is often simply to manage efficient and swift flows of goods, people and information.[44] However, what spells ‘efficiency’ for one person spells ‘social control’ for another: this is particularly true for strongly personalised systems like ID records retrieval, which involves consistent and unique identifiers for individual citizens.[45]

Information Sharing: 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.[46] 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.[47] This is the case in public services, law enforcement, border management and marketing. For example, 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.[48]

The Blurring of Public / Private Boundaries: Whilst both public sector and private sector share information, boundaries between state and private sector interests are blurring, as more tasks of government are carried out through a sometimes complex combination of public, private, voluntary-sector and market mechanisms. 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.[49] 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. Questions will continue to be raised with the privatisation of telecommunications, border management (IBM’s Project Semaphore, the UK’s e-borders programme) and local security (e.g. Citizen Corps in the US who ‘look out for unusual activities’).

Social Consequences of Surveillance

We now turn more overtly to the social consequences of the surveillance technologies and processes we have just discussed. 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. We would also emphasise the far less frequently

[43] Lianos, M. (2001) *Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social.* Paris : L’Harmattan-Logiques Sociales.

[44] Graham, S. and Wood, D. (2003) ‘Digitising surveillance: categorisation, space and inequality,’ *Critical Social Policy*, 23: 227-248.

[45] 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

[46] 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.

[47] A recent Home Office consultation paper, 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’.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, with a remit to ‘develop the Government's strategy on data-sharing across the public sector’.

[48] Evans, M. (2005) ‘The data-informed marketing model and its social responsibility.’ in Lace, S (2005) *op cit.*, n.3.

[49] 6 *et al.* 2005 *op cit.* n.24; Bellamy *et al.*, 2005 *op cit.* n.46.

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.

Autonomy: Anonymity and Privacy: Surveillance affects autonomy by compromising individual anonymity and privacy. In many ways, a general condition of anonymity allows the individual the ability to make their own identity through their actions and relationships. 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. The privacy of the vulnerable or marginalised is continually diminishing. In UK prisons, offenders all subject to almost constant surveillance. Even once released from prison, offenders are also increasingly subjected to electronic monitoring either as a condition of early release from prison under the Home Detention Curfew Scheme[50] or as a condition of being released on parole.[51] Employers' capacities to delve into the private lives of their employees must be continually scrutinised. The coverage of multiple databases by national identification systems, particularly those which span public and private sectors, is a key area of concern. Similarly 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.[52]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'.[53]

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. 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 choice can be seen at work throughout the criminal justice system. We do not choose to be monitored by CCTV as we walk though public space, and no one has chosen to have their vehicle movements logged at the ACPO's ANPR Centre. Arrestees do not choose, 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. 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.

Discrimination: Speed, Access and Social Exclusion: 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. 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.[54] Those

[50] 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.

[51] *ibid.*

[52] 'Phone firms 'flooded' by crime checks'. *BBC News*, 20 December 2002, http://news.bbc.co.uk/1/low/uk/2592707.stm

[53] Stanley, J. (2004) *The Surveillance-Industrial Complex*, Washington DC: ACLU. http://www.aclu.org/FilesPDFs/surveillance_report.pdf

[54] Bigo, D. (2004) 'Globalized in-security: the field of the professionals of unease management and the ban-opticon,' *Traces*, 4.

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.

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. Once introduced, however, both access and blockage are increasingly policed automatically,[55] 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. Exclusion is also 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. And 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 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, because e-recruitment is subject to biases and ‘rules of thumb’ embodied in professionals’ choice of keyword search term, [56] [57] and second, because certain social, economic and ethnic groups do not have easy access to the internet.

This can work itself deep into the very infrastructure of society. With human discretion removed and embedded in code, and 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.

Democracy, Accountability and Transparency: 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.

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

[55] 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 .

[56] Tversky, A. and Kahneman, D (1974) ‘Judgement under uncertainty: heuristics and biases,’ *Science* 185(4157): 1124-1131

[57] Mohamed, A.A., Orife, J. and Wibowo, K. (2002) ‘The legality of key word search as a personnel selection tool,’ *Employee Relations* 24(5).

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.

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.

4. Regulating the Surveillance Society

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[58]: that is, they apply rules to surveillance and data processing by setting limits and controls. Most of the systems for controlling personal data information processing 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. 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. In this section of the Report we reflect on the regulatory experience, and assess the adequacy of these efforts. We also suggest possibilities for improvement.

What is Wrong with Regulation?

Regulation of privacy and surveillance has suffered from some common drawbacks. We are able to identify at least six areas of difficulty:

- Regulation has tended to be reactive: 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’.

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

- Regulation has been discussed and implemented largely outside of public debate. Debate has taken place within expert communities: for example, the world of data 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. 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’.

The Current State of Regulation

For the past thirty-five or more years, privacy protection has spread round the world. Lying at the heart of these developments have been some totemic principles. 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*;
- 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.[59]

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 Directive on Privacy and Communications (2002/58/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

[59] Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge MA: MIT Press, 12.

adopted privacy statements or policies. 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.

Building a practical system to control surveillance on the slender foundation of information privacy protection seems, to many, to be misguided. To others,[60] 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. New surveillance practices, however, 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 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.

Regulatory Instruments: Pros and Cons

The existing repertoire of policy instruments that have been brought into use for privacy and data protection, and therefore apply to large areas of surveillance as well are as follows:[61]

International instruments: 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. These and related documents have shaped specific legislative and implementation activity in a very large number of countries and lesser jurisdictions. Action at the international level is largely responsible for the pre-eminence of the set of principles that have governed data protection, and by extension, surveillance, for a long time.

Laws: The global spread of legislation 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, 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. The weakness of many laws and their implementation machinery in the field of personal information processing has long been a matter for complaint. Critics may have reason for impatience with legal solutions that may legitimate surveillance rather than regulate it.[62] 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. In addition, the harm that surveillance may do to individuals, groups

[60] e.g.: Dubbeld, L. (2004) *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance.* Enschede: Ipskamp Printpartners.

[61] For a more detailed typology and discussion, see *op cit.* n. 59: chs. 4-7.

[62] 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.

and whole societies do not come within the range of impacts that these individual rights-based laws are designed to remedy or prevent.

*Self-regulation***:** 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. There are also online means of self-regulation by merchants who trade over the Internet, in the form of online privacy statements, 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. Self-regulation is increasingly regarded as a better way of regulation given the 'failure' of laws and the less-regulated business climate that is considered desirable to foster.[63] 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.

Privacy-enhancing technologies: A major development since the early 1990s has been the realisation that technologies themselves can provide powerful controls over surveillance or privacy invasion. Hence, the surveillance or non-surveillance potentials of specific technologies depend upon how they are designed and deployed. Thus 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.[64] Encryption, anonymous web-browsing, filtering devices, smart agents, privacy-preference tools and the like may act as empowering instruments for the individual. It is unclear whether they are strong solutions to online surveillance practices by themselves.

*Individual self-help***:** This is a further broad category of regulation. Here, the individual controls their own information disclosure, either through the use of PETs, by opting-in or opting-out of certain information-processing procedures, but also through knowledge, awareness and vigilance concerning the surveillance practices and privacy threats. All these put a premium on the individual having sufficient interest in protection and the 'cultural capital' – the ability and the means to comprehend what is happening, and to assert themselves 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.

We would also identify the activities of the following as important:

- 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.

[63] 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.

[64] Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York NY: Basic Books.

General Problems Concerning Instruments

Three of the most important problems with existing regulatory practices 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 difficulty concerns 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. 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.

Options for Future Regulation

Privacy Impact Assessment: 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.[65] PIA may best be seen as an instrument that those who proposing new or revised personal data-processing systems can use to mitigate the potentially harmful privacy effects on data subjects. 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, such as better, more citizen-oriented public service, or security, and not as an obstacle to them.

From Privacy Impact Assessment to Surveillance Impact Assessment: To encompass the potentially harmful effects of surveillance on a wider basis than that of protecting privacy, we suggest 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.

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.[66] 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. 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 ones privacy protected. It is a collective value insofar as it is 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.[67] This is why SIA could play a valuable role by incorporating PIA but transcending it with a range of enquiries aimed at assessing the

[65] 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.
[66] Regan (1995) *op cit.* n.9, ch. 8.
[67] *ibid.*

impact of surveillance, or privacy invasion, upon society itself and upon the other, non-privacy, interests of separate individuals, categories and groups.

Questions raised in a SIA might include:[68]

- Does the technique cause unwarranted physical or psychological harm?
- Does the technique cross a personal boundary without permission (whether involving coercion or deception or a body, relational, or spatial border)?
- Does the technique violate assumptions that are made about how personal information will be treated, such as no secret recordings?

*Other Options***:** If SIA builds upon PIA, other options also build upon the present.

- Build a pool of technological knowledge-and-awareness capability to help regulators stay abreast of technological developments.
- Advise managers and technologists on how to design implement surveillance techniques responsibly, paying particular attention to strategy, organizational change, staff training and social responsibility
- Reconceptualise privacy as a collective social value, rather than an individual value.
- Encourage public debate about surveillance in a participative and non patronising way
- Conduct independent assessments of the costs of privacy, surveillance regulation and compliance. Consider whether they are excessive, and whether they inhibit innovation. Consider whether this balances the benefits of public trust and efficiency, bearing in mind that the ‘balance’ test is far from adequate and should be scrutinised in itself.
- Elevate the tone of the media beyond clichés, sensationalism and scare-mongering

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. 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. 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.

[68] Gary T. Marx, ‘Ethics for a the New Surveillance’, *The Information Society*, 14, 3, 1998: 174