Surveillance Society

David Lyon, Queen's University, Canada

Talk for Festival del Diritto, Piacenza, Italia: September 28 2008

What is the Surveillance Society?

We live in a surveillance society. The arrival of "surveillance society" is no longer 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 and normally we take this to be unremarkable.

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 also 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. Surveillance is part of the way we run the world in the twenty-first century.

Conventionally, to speak of surveillance society is to invoke something sinister, smacking of dictators and totalitarianism. But the surveillance society is better thought of as the outcome of modern organizational trends in workplaces, businesses and the military than as a covert conspiracy. Surveillance, seen as the growing role of information within large-scale bureaucratic organizations – may be viewed as progress towards efficient administration. As the sociologist Max Weber pointed out early in the twentieth century, bureaucracy is regarded as a benefit for the development of Western business and modern government.[1]

Some forms of surveillance have always existed as people watch over each other both for mutual care and for moral caution. However, from about 400 hundred years ago, 'rational' methods began to be applied to organizational practice, that steadily did away with many 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.

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

Impersonal and rule-centred practices spawned surveillance. Essential to this is the oversight of subordinates within the system, and the creating and maintaining of records, usually involving personal data both on employees and on those whose needs and claims are being administered. 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.

What is wrong with surveillance society?

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 bureaucratic organizational practices 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.

Surveillance is two-sided, and the benefits of correct identification, screening, checking, appropriate classification and other tasks associated with it must be acknowledged. At the same time risks and dangers are always present in large-scale systems and power does corrupt or at least skews the vision of those who wield it.

Take risks and dangers first. These are something we have become more used to since the public realization 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] 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.

It is equally important, secondly, to remember the point about the corruptions and skewed visions of power. Again, we do not have to imagine some wicked tyrant 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 or making children safe from predators) to justify unusual or extraordinary tactics.

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. What exceptional circumstances justify mass fingerprinting of Roma people in Italy?

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, we are told, corporations need to amass personal data on a grand scale. Then they will '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 (in the UK). 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]

What else is wrong with surveillance society? One (following from what was said about exceptional circumstances and unintended consequences): Surveillance permits 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.

Two, today's surveillance processes and practices bespeak a world where we know we are not really trusted. Surveillance fosters suspicion and thus threatens social cohesion and solidarity.[7] The employer who installs keystroke monitors at workstations, or GPS devices in service vehicles is saying in effect that he does not trust his employees. The welfare benefits administrator who seeks evidence of double-dipping or solicits tipoffs on a possible 'spouse-in-the-house' is saying she does not trust her clients. And when parents start to use webcams and GPS systems to check on their teenagers' activities, they are saying they do not 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.

Three, surveillance distracts from alternative methods and from larger and more urgent questions. This is especially so when surveillance is associated with high technology and anti-terrorism, and other policy preoccupations. Is more surveillance 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.

Defining surveillance; tracing surveillance society

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.

To break that 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 is 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.

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, created in bureaucratic organizations and referring to transactions, exchanges, statuses, accounts and so on, Roger Clarke calls 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 act as incentives to extend the system even though the data are not strictly required for the original purpose.

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 mobile phones to find out about each others' activities (and again, trust has eroded in such cases), and watching from below -- or 'sousveillance' -- may also occur when ordinary people grasp the cameras and watch the watchers.[9]

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]

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 again, 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.

What neither Kafka nor Orwell could have foreseen was the rise of computers and the wholesale digitizing of administration. After all, the 'silicon chip,' on which device the information revolution was based, 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 occurs. While the dilemmas of surveillance are brilliantly explored in *The Conversation* (1974) and in *The Lives of Others* (2006) these rely primarily on conventional audio-surveillance and eavesdropping. Other 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.

This is why we need the social sciences. 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 only as evidence of 'progress,' but as deeply ambiguous. At worst, he predicted that the efficient but soulless world of new organizational methods in every sphere 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' at the level of government and you have a recipe for repression as well.

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 business firms, communications and even entertainment (indeed, *Big Brother* as 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.

Where exactly we go beyond Weber is unclear. Michel Foucault's stimulating reflections on surveillance open up many fascinating and illuminating avenues of enquiry. While the panopticon may not be the best model, understanding discipline as surveillance throws light on the processes. Others such as Deleuze have suggested that today we're beyond the fixed and closed spaces of the panopticon and must consider surveillance in much more fluid ways. The motif of control is now dominant, as ordinary people have to identify themselves and present credentials continually in everyday life. Protocols govern many choices and chances in daily existence.

1. Situating Surveillance Society

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.

The issues:

a. 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 'Fair Information Principles' (FIPs) 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[13] 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 is wrong, identify what it is and know where to take the complaint and how to find redress.

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, 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:

b. 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. It is not because of surveillance, of course, that the nation-state today feels it can no longer offer the kinds of social security that it once aspired to, or that it now downscales its aims to providing only some forms of basic individual safety.[14] Rather, surveillance grows alongside these changes, usually supporting or at least enabling them. As well, the agencies of individual safety can easily be outsourced.

Cradle-to-grave health-and-welfare, once the proud promise of social-democratic governments, has been whittled down to risk management and – here is where the surveillance society comes in – such risk management demands full knowledge of the situation. So data – personal data – are sought in order to know where to direct resources.[15] 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 are that frequently police hot-spots are predominantly in non-white areas, and supermarkets are located in upscale neighbourhoods easily reached by those with cars.

c. Choice, power and empowerment

So what say do ordinary citizens, consumers, workers and travelers have in shaping the surveillance society? Again it must be 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.

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[16] and 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 specialized 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.

d. Transparency, accountability

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 organizations 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 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 obtaining negotiated consent for it from the employees. When it comes to consumer surveillance, however, not 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 minimizing of surveillance.

The Processes:

a. Social sorting

In the surveillance society, social sorting is endemic. In government and commerce large personal information databases are analyzed and categorized to define target markets and risky populations.[17] Amazon.com, for example, 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 is concerned, you are their profile. Amazon 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.

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 far as urban infrastructure in concerned, 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.

b. 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 (as the section on public services indicates). Yet there is already scarce 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. 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 harmonization of 'intelligence-led' systems seems to be both technologically and administratively desirable.

c. Function creep

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.[18] 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.

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 organizational efficiency is frequently seen as a top priority, the human consequences of function creep are all-too-often unknown, ignored or downplayed.

d. Technologies

Surveillance today is often thought of only in technological terms. Technologies are indeed crucially important, but two important things must also be remembered: One, 'human surveillance' of a direct kind, unmediated by technology, still occurs and is often yoked with more technological kinds. Two, technological systems themselves are neither the cause nor the sum of what surveillance is today. We cannot simply read surveillance consequences off the capacities of each new system (especially if those capacities are described by the vendor). If technologies are indeed important for surveillance, how should they be viewed?

For the surveillance society properly to be understood, technologies should be analyzed 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 organization. Moreover, we need to understand these things clearly enough to influence policy and practice. Impacts assessments are one way.

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. Also, national ID card systems create huge new developments of joined-up surveillance. One important implication is that those – workers, consumers, claimants, citizens, patients, academics and so on as well as data protection professionals -- 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.

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. The real world of surveillance society is far to complex for such superficial responses.

[1] Hans Gerth and C. Wright Mills, *From Max Weber*, New York, 1946.
[2] Ulrich Beck, *The Risk Society*, London: Sage.
[3] See Anthony Barbaro and Tom Zeller, 'A face is exposed for AOL searcher no. 4417749' *New York Times*, August 9, 2006. Archived at http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/
[4] See Amnesty USA report on racial profiling, 2004, at www.amnestyusa.org/racial_profiling/report/index.html/
[5] See http://www.washingtonpost.com/ac2/wp-dyn/A20199-2004Aug20?language=printer
[6] See Susanne Lace, *The Glass Consumer*, Bristol UK: Policy Press 2005; Anthony Danna and Oscar Gandy, 'All that glitters is not gold: Digging beneath the surface of data-mining' *Journal of Business Ethics*, 40, 2002: 373-386; David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York: Routledge, 2003.
[7] This is discussed in David Lyon, *Surveillance after September 11*, Cambridge UK: Polity Press, 45-48, 142ff.
[8] Clarke Roger 1997 'Introduction to dataveillance and information privacy', available at www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV [revised August 7 2006].
[9] Steve Mann, Jason Nolan and Barry Wellman. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1(3) 2003: 331-355.
[10] Such as James Rule *Private Lives, Public Surveillance*, London: Allen Lane, 1973. The best-known in the 1980s were probably David Burnham, *The Rise of the Computer State*, New York: Vintage Books, 1983 and Gary T. Marx *Undercover: Police Surveillance in America*, Berkeley: University of California Press, 1988.
[11] Gary T. Marx, 'The surveillance society: the threat of 1984-style techniques' *The Futurist*, June 1985, 21-26; Oscar Gandy, 'The surveillance society: information technology and bureaucratic social control' *Journal of Communication*, 39:3, 1989.
[12] See John McGrath, *Loving Big Brother*, London: Routledge 2004; Mark Andrejevic, *Reality TV: The Work of Watching*, Rowman and Littlefield 2004.
[13] See the excellent treatment of the sociality of privacy in Priscilla Regan, *Legislating Privacy*, Chapel Hill: University of North Carolina Press, 1995.
[14] See e.g. the discussion in Zygmunt Bauman, *Liquid Fear*, Cambridge UK: Polity Press.
[15] See Richard Ericson and Kevin Haggerty, *Policing the Risk Society*, Toronto: University of Toronto Press, 1997.
[16] See the *New York Times* editorial on 'The data-fleecing of America' June 21, 2005.
[17] See Oscar Gandy's classic study, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview, 1993.
[18] See 'Oyster data use rises in crime clamp-down' *The Guardian*, March 13 2006, available at http://politics.guardian.co.uk/foi/story/0,,1730771,00.html/