

## **Surveillance, Power and Everyday Life**

David Lyon

A chapter for the *Oxford Handbook of Information and Communication*

*Technologies*

Abstract

Surveillance has become a crucial component of all environments informed or enabled by ICTs. Equally, almost all surveillance practices in technologically 'advanced' societies are enhanced and amplified by ICTs. Surveillance is understood as any focused attention to personal details for the purposes of influence, management, or control. Thus in addition to those who may be 'suspects' (because of alleged offences), ordinary persons in everyday life – workers, consumers, citizens, travellers -- find that their personal data are of interest to others. Agencies process personal data in order to calculate risks or to predict opportunities, classifying and profiling their records routinely. While everyday life may thus seem less 'private', and ordinary people may feel that they are more vulnerable to intrusion, the use of searchable databases for categorizing and profiling means that deeper questions of power are involved. Life chances and choices are affected – sometimes negatively – by the judgments made on the basis of concatenated data, which means that such surveillance is implicated in basic questions of social justice, to do with access, risk distribution and freedom. There is increased need for ethics and politics of information in an era of intensifying surveillance.

### **Introduction**

Surveillance grows constantly, especially in the countries of the global north.

Although as a set of practices it's as old as history itself, systematic surveillance became a routine and inescapable part of everyday life in modern times and is now, more often than not, dependent on information and communication technologies (ICTs). Indeed, it now makes some sense to talk

of 'surveillance societies,' so pervasive is organizational monitoring of many kinds. Fast developing technologies combined with new governmental and commercial strategies mean that new modes of surveillance proliferate, making surveillance expansion hard to follow, let alone analyse or regulate.

In the past three decades traffic in personal data has expanded explosively, touching numerous points of everyday life and leading some to proclaim the 'end of privacy'. But while questions of privacy are both interesting and important (see Raab, this volume), others that relate to the ways in which data are used for 'social sorting', discriminating between groups who are classified differently, also need urgently to be examined. Who has the power to make such discriminatory judgements, and how this becomes embedded in automated systems, is a matter of not merely academic interest. Such questions are likely to be with us for some time, both because of what might be called the 'rise of the safety state' that requires more and more surveillance, and also because the politics of personal information is becoming increasingly prominent.

Literally, surveillance means to 'watch over' and as such it is an everyday practice in which human beings engage routinely, often unthinkingly. Parents watch over children, employers watch over workers, police watch over neighbourhoods, guards watch over prisoners and so on. In most instances, however, surveillance has a more specific usage, referring to some focused and purposive attention to objects, data, or persons. Agricultural experts may do aerial surveillance of crops, public health officials may conduct medical

surveillance of populations, or intelligence officers may put suspects under observation.

Such activities have several things in common, among which are that in today's world some kind of technical augmentation or assistance of surveillance processes is often assumed. ICTs are utilized to increase the power, reach and capacity of surveillance systems. The specific kind of surveillance discussed here is perhaps the fastest growing and almost certainly the most controversial, namely the processing of personal data for the purposes of care or control, to influence or manage persons and populations. In this and every other respect, power relations are intrinsic to surveillance processes.

This being so, it immediately becomes apparent that actual 'watching over' is not really the main issue, or at least not literally. While CCTV (Closed Circuit Television) surveillance certainly does have a watching element, other kinds of ICT-enabled surveillance include the processing of all kinds of data, images and information. Ones of which we are most aware include the multiple checks which we go through at an airport, from the initial ticketing information and passport check through to baggage screening and the ID and ticket check at the gate. In this example, both public (governmental; customs and immigration) and private (commercial; airlines and frequent flyer clubs) data are sought. Others of which we may be less consciously aware include 'loyalty cards' at supermarkets and other stores, which offer customers

discounts and member privileges, but that are simultaneously the means of garnering consumer data from shoppers.

All these count as surveillance of one kind or another, in which we are (usually) individuated – distinguished from others, identified – according to the criteria of the organization in question, and then some sort of analysis of our transaction, communication, behaviour or activity is set in train. Thus some kinds of surveillance knowledge are produced that are then used to mark the individual, to locate him or her in a particular niche or category of risk proneness, and to assign social places or opportunities to the person according to the ruling criteria of the organization. It is not merely that some kinds of surveillance may seem invasive or intrusive, but rather that social relations and social power are organized in part through surveillance strategies.

It should be noted that surveillance involving direct watching or monitoring continues to be an important part of social life, but the kind of surveillance discussed here is supported, enabled, or assisted by ICTs. In the later part of the twentieth century the idea became popular that ‘information societies’ were in the making, wherever computer and telecommunication technologies formed essential infrastructures for administrative and organizational life. Although a certain technological determinism drove some of these ideas – after all, paper file-based bureaucracies created ‘information societies’ long before vacuum tubes, transistors or silicon chips had been invented – the notion that significant changes occurs with the use of digital infrastructures

should not simply be discounted. One of the key changes is that routine, mundane, everyday surveillance is enabled by those infrastructures. Indeed, one can argue that the 'surveillance societies' of today are a by-product of the so-called 'information society'.

## **Surveillance Society**

From time-to-time social scientists propose labels and phrases that highlight crucial aspects of contemporary change and 'surveillance society' is one of these. First used by sociologist Gary T. Marx in the mid-1980s (Marx 1985, see also Gandy 1989), the phrase is now in common use, frequently by those who wish to make the same kinds of points as Marx did then. His concern was that new technologies were helping to create situations in which 'one of the final barriers to total social control is now crumbling'. Soon afterwards, historian David Flaherty commented that Western countries in general were becoming surveillance societies, '...as one component of becoming information societies' (Flaherty 1989:1). Two decades later, in 2004, the British Information Commissioner, Richard Thomas, warned that with the proposed introduction of a national identification card the UK was in danger of sleepwalking into a surveillance society (*Times* [London], 28 August 2004).

What kinds of processes would have to be in place to warrant the use of a phrase like 'surveillance society'? For Richard Thomas, the issue was that the UK government would be enabled through the 'Citizens' Information Project' of the Office of the Census to collect far more personal data than is necessary

for the purposes of the ID card. At the same time, he questioned what exactly is the main purpose of the proposed card – to regulate immigration, to combat terrorism or to provide access to services and benefits? For Thomas, the surveillance society clearly relates to state activities (rather like *Nineteen-Eighty-Four* perhaps) that are augmented by the use of new technologies – the Citizens' Information Project is a national database. He also referred to twentieth century examples of state rule by surveillance, such as in older Eastern European societies and Franco's Spain.

A similar kind of analysis, though more rigorously sociological, was made by James Rule in the early 1970s, when he suggested that an 'ideal type' -- a 'total surveillance society' – be imagined, by which to judge increases in surveillance. Surveillance capacities were rapidly being expanded, he showed, through the use of computerization that permitted increasing file size, greater centralization, higher speeds of data flow between points in the system and the number of contact points between the system and the subject (Rule 1973:37-40). While Rule's studies related in part to government administration, in the form of drivers' licences, national insurance and policing in the UK, he also studied consumer credit reporting and credit cards systems in the USA. Already, then, hints of a surveillance *society* rather than just a surveillance *state* were becoming visible. And with it came new forms of power, of subtle shifts in governance.

This is the point of considering the surveillance *society*. What was once thought to refer primarily (and perhaps mistakenly) to affairs of state now has

become societally pervasive. Surveillance, assisted by new technologies, appears in everyday commercial life, as people pay with credit cards and as their shopping habits are monitored through credit reporting. Today, however, this process is vastly magnified, such that all manner of everyday activities are recorded, checked, traced and monitored for a variety of purposes. Consumers are profiled by corporations as never before, and several new technical developments such as the internet and cell phones, unknown to Rule and others in the 1970s and 1980s, make available new thick layers of surveillance data.

Once advantage of thinking in terms of a surveillance *society* is that this term deflects attention from other models of how surveillance works. The main such models are the Orwellian apparatus of a totalitarian state, depicted in the novel *Nineteen-Eighty-Four* and Jeremy Bentham's penitentiary plan for a 'Panopticon' or 'all-seeing place'. The former formed the starting point for several sociological studies (such as James Rule's) whereas the latter became the centrepiece of Michel Foucault's study of discipline in the modern world. The point is not to dismiss these models as to place them in a larger context.

The idea that state power could be augmented by surveillance systems in ways that are at least reminiscent of totalitarianism is quite plausible. This may be seen in some south-east Asian countries such as Singapore and also in western societies such as the USA, following the attacks of 9/11 (Lyon 2003, Ball and Webster 2004). And the analysis of self-discipline, induced by

the uncertainty and fear associated with unseen observers, within a closed environment such as a prison, but also in more public venues, does give the panopticon considerable credibility. There is evidence that people do alter their behaviours when, for instance, they are aware that they are under video surveillance (Norris and Armstrong 1999, McCahill 2002, Cole 2004). These forms of analysis have not simply been superseded. Rather they are inadequate on their own.

There is much more to contemporary surveillance than totalitarianism or panopticism, significant though these concepts are. Several writers have pointed to other features of surveillance that are difficult to squeeze into either of those frames. Gilles Deleuze, for example, suggested in a brief statement on 'societies of control' that we all now live in situations where 'audio-visual protocols' – such as cameras, PINs, barcodes, RFIDs -- help to determine which opportunities are open, and which closed, to us in daily life (Deleuze 1992). His (and Felix Guattari's) idea of the 'assemblage' of surveillance activities has also been taken up by a number of sociological authors (such as Ericson and Haggerty 2000).

The notion of assemblage in this context points to the increasing convergence of once discrete systems of surveillance (administration, employment, health, insurance, credit and so on) such that (in this case) digital data derived from human bodies flows within networks. At particular points the state, or totalizing institutions such as prisons, may focus or fix the flows to enable control or direction of the actions of persons or groups. But in this view surveillance



becomes more socially levelled out, non-hierarchical, and inclusive of others who might once have felt themselves impervious to the gaze. At the same time, it is suggested, surveillance itself will not be slowed merely by resisting a particular technology or institution.

Others, sometimes indirectly, have also proposed fresh ways of examining surveillance beyond those classic foci on the 'state' or total institutions as its perpetrators. Nikolas Rose, for instance, argues that surveillance be seen as part of contemporary governmentality, the way that governance actually happens, rather than thinking of it as an aspect of institutional state activities. Modern systems of rule, says Rose, depend on a complex set of relationships between state and non-state authorities, infrastructural powers, authorities that have no 'established' power and networks of power (Rose 1996:15). Surveillance, that pays close attention of personal details, especially those that are digitally retrievable, contributes to such governmentality. Indeed, it may, paradoxically, use 'freedom' (conventionally considered in opposition to state power) to further its ends. Consumer 'freedom' and surveillance is a case in point.

Perspectives such as Rose's offer much to critical thought. The powers of which he writes, expressed in part through surveillance, now spill over the territories once associated with the nation-state. In their work on 'empire', Richard Hardt and Antonio Negri argue that surveillance is effectively globalized and indeed is vital to new regimes of imperial power (Hardt and Negri 2000). Moreover the ways that contemporary surveillance works leads

to new forms of exclusion (rather than control through inclusion that was characteristic of Foucault's understanding of the Benthamite Panopticon). This is clear from empirical studies (such as Norris 2003 on public CCTV), Bauman (2000) on super-max prisons and also from the theoretical work of Giorgio Agamben (that criticizes Foucault for never demonstrating *how* 'sovereign power produces biopolitical bodies', Agamben 1998).

Such exclusionary power has come more clearly into focus since 9/11, not only in the attempts to identify 'terrorists' and to prevent them from violent action, but also in the more general sorting of foreign workers, immigrants and asylum seekers into 'desirable' and 'undesirable' categories. As Bigo and Guild (2005: 3) say, while Foucault thought of surveillance as something that affects citizens equally, in fact '...the social practices of surveillance and control sort out, filter and serialize who needs to be controlled and who is free of that control...' Such sorting is becoming increasingly evident not only in Europe but in North America and elsewhere too. And it is facilitated by new surveillance measures such as biometric passports and electronic ID cards, currently being established in the UK and the USA (Lyon 2004).

The notion of a surveillance society is also given credence by the fact that in ordinary everyday life not only are people constantly being watched, they are also willing, it seems, to use technical devices to watch others. Plenty of domestic technologies are on the market, for providing video camera 'protection' to homes; CCTV is commonplace in schools and on school buses, and many schools are adopting automated identification systems; spouses

may use surreptitious means to check on each other, and there is a burgeoning trade in gadgets with which parents may 'watch' their children. Day Care cams permit parents to see what their toddlers are up to, Nanny cams monitor for suspected abuse and cell phones are often given to children so that their parents may 'know where they are'. Those technologies that originated in military and police use and later migrated to large organizations and government departments may now be used for mundane, civilian, local and familial purposes.

At the same time, the broader frames for understanding surveillance, such as governmentality, that acknowledge its ambiguity as well as its ubiquity, permit consideration of how new technologies may also empower the watched. While global imperial power is undoubtedly stretched by surveillance, and social exclusion is automated by the same means, internet blogs, cell-phone cameras and other recent innovations may be used for democratic and even counter-surveillance ends. While such activities have none of the routine and systematic character let alone the infrastructural resources of most institutional surveillance they may nevertheless contribute to alternative perspectives and to the organizational capacities of counter-hegemonic social movements.

### **Surveillance Technologies**

The very term 'surveillance technologies' is somewhat misleading. If one visits the 'spy stores' that seem to spring up in every city, the term seems clear

enough. You can purchase disguised video cameras, audio surveillance and telephone tapping equipment, GPS (Global Positioning Satellite) enabled tracking devices and of course counter-surveillance tools as well. But each of these is intended for very small-scale use – usually one surveillor, one person under surveillance, and they are often people already known to each other – and is decidedly covert. In policing and other investigative activities, such specifically targeted and individually triggered surveillance may be called for, but the kinds of surveillance discussed here are different in almost every respect. In terms of power relations, individual surveillance is one thing; institutional surveillance is quite another.

Surveillance that has developed as an aspect of bureaucratic administration in the modern world (see Dandeker 1990) is large-scale, systematic, and now is increasingly automated and dependent on networked computer power. It depends above all on searchable databases (Lessig 1999) to retrieve and process the relevant data. Although some systems depend on images or film (such as CCTV), even these possess far greater surveillance power when yoked with searchable databases. And in most cases surveillance is not covert. It is often known about, at least in a general way, by those whose data are extracted, stored, manipulated, concatenated, traded and processed in many other ways. Those buying houses are aware that checks will be made on them, patients know that health care agencies keep detailed records, video surveillance cameras are visible on the street, internet surfers know their activities are traced and so on. We return to this point below.

Surveillance technologies enable surveillance to occur routinely, automatically, but only in some cases is the surveillance aspect primary. Clearly, the point of public CCTV is to 'keep an eye' on the street or train station (although even here the larger goal may be public order or maximizing consumption). In the UK, there are more than 4 million cameras in public places (Norris and McCahill 2004). Police and intelligence services also use technologies such as fingerprinting devices, wiretaps, CCTV and so on for surveillance purposes and all these depend (or are coming to depend) on searchable databases. For this reason, among others, they contribute to qualitatively different situations, sometimes amounting to a challenge to traditional conceptions of criminal justice (Marx 1988, 1998). In many cases, however, surveillance is the by-product, accompaniment or even unintended consequence of other processes and practices. It is sometimes not until some system is installed for another purpose that its surveillance potential becomes apparent.

Marketers claim that they 'want to know and serve their customers better' and this entails finding out as much as possible about tastes, preferences and past purchases, which has now developed into a multi-billion dollar industry using Customer Relationship Marketing (CRM; see 6: 2005). Retailers may install ceiling mounted cameras in stores to combat shoplifting only to discover that this is also a really good way of monitoring employees as well. In the 'privacy' field this latter process is often referred to using Langdon Winner's phrase, 'function creep' (Winner 1977). Winner, like David Thomas almost thirty years later, warned that once a digitized national ID number has

been assigned – say, to combat terrorism -- its use is likely to be expanded to cover many cognate areas.

Whatever the specific characteristics of surveillance technologies, they also have to be located culturally in certain discourses of technology. Especially in the western world and above all in the USA, technology holds a special place in popular imagination and in public policy. Technical ‘solutions’ to an array of perceived social, economic and political questions are all-too-quickly advanced and adopted, particularly in the aftermath of some crisis or catastrophe. This is not the start of an anti-technology argument – I have already claimed that surveillance is in part a necessary aspect of the technology-enhanced administrative and organizational regimes that have ordered social life for more than a century in the west -- but rather an observation that technical responses have become commonplace, taken for granted.

In the mid-twentieth century Jacques Ellul famously insisted that in the ‘technological society’, *la technique*, or the ‘one best way of doing things’ had become a kind of holy grail, especially in the USA. In a world where from the late nineteenth century ‘progress’ associated with undeniable technological advancement (at least in some domains) had been proclaimed, to fall back on technical solutions was both understandable, straightforwardly manageable and, of course, lucrative for the companies concerned. By the end of the twentieth century Robert Wuthnow, a sociologist of religion, could argue that technology remains one of the few beliefs that unites Americans (1998). And if

it was not clear before the twenty-first century, the challenge of terrorism certainly made it clear that technical responses were highly profitable. Share prices in security and surveillance companies surged after the attacks of 9/11 and also after the Madrid (2003) and London (2005) bombings (see, e.g. siliconvalley.com July 7 2005). The political economy of surveillance should not be overlooked; technology companies constantly press for procurements.

The steady and often subtle adoption of new technologies – including surveillance devices and systems -- into everyday life is highly significant from a sociological point of view. If it was ever appropriate to think of social situations in a technological vacuum those days are definitely over. Because, for example, machines such as cell phones and computers have become essential for so many everyday communications, analyses of networks of social relations cannot but include reference to them. This is the ‘technoculture.’ Frequently, however, the focus is on how fresh forms of relationship are *enabled* by the new technologies rather than on how power may also be involved in ways that *limit or channel* social activities and processes. In a post- 9/11 environment, the main things that come to mind in this connection may be the threats to civil liberties from the hasty deployment of supposedly risk-reducing technologies in the name of national security. But equally, the mundane activities of shopping using credit and loyalty cards may also contribute to profoundly significant processes of automated social sorting into newer spatially-based social class categories that modify older formations of class and status. Sociology itself is obliged to readjust to such shifts (see Burrows and Gane forthcoming).

## **The explosion of personal data**

It is difficult to exaggerate the massive surge in traffic in personal data from the 1970s to today. And the quantitative changes have qualitative consequences. It is not merely that more and more data circulate in numerous administrative and commercial systems, but that ways of organizing daily life are changing as people interact with surveillance systems. One of the biggest reasons for this is hinted at in the word that I just used to describe it -- 'traffic.' There is constant growth in the volume of personal data that flow locally, nationally and internationally through electronic networks. But one cause of this is 'traffic' in another, economic, sense, in which personal data are sought, stored and traded as valuable commodities.

Long before notions of the 'surveillant assemblage' came to the fore, Australian computer scientist Roger Clarke had proposed another term to capture the idea of 'surveillance-by-data': 'dataveillance' (Clarke 1988, but cf. Genosko forthcoming). A surge in surveillance could be traced, he argued, to the convergence of new technologies – computers and telecommunications – that rendered Orwell's ubiquitous two-way television unnecessary. The novel combinations made possible by ICTs permitted quite unprecedented flows of data, illustrated by Clarke in the case of EFT or 'Electronic Funds Transfer'.



It is hard for those who now assume the constant networks of flows (the term is Manuel Castells') to recall how revolutionary EFT seemed at the time. It enabled supermarket shoppers, for instance, to have their accounts conveniently debited at the point of sale, thus bypassing several stages of financial transaction that would previously have had to occur. Such transfers are not only now commonplace, they also occur across a range of agencies and institutions that once had only indirect and complex connections. Clarke's point about *Nineteenth-Eighty-Four* was a critical one, pointing to the potentially negative surveillance capacities of dataveillance. Without minimizing that point, however, it is crucial to note that the major difference between the two is that EFT and its descendants are not centralized. Indeed, to the contrary, they are diffuse, shifting, ebbing and flowing – and yet as we shall see, not without discernible patterns of their own.

Even when Clarke was writing about dataveillance, a further innovation had yet to become a household word. What is often referred to as the 'internet' (meaning a range of items, usually including email systems and the World Wide Web) was only coming into being as a publicly accessible tool in the early 1990s. The debate over its threatened commercialization was hot; until then it was the preserve of the military, academics and computer enthusiasts, many of whom saw it as an intrinsically open medium. Its eventual role as a global purveyor of information, ideas, images and data, under the sign of consumerism, signals a major augmentation of surveillance.

Not only were computers and communications systems enabling new data-flows of many kinds, now consumers could participate directly in the process. Online-purchasing of goods and services from groceries to airline tickets to banking meant that personal data was moving on a massive scale. Who had access to these data, and how they could be secured and protected became a central question as quite new categories of crime appeared, such as 'identity theft', and as corporations fell over themselves to gain access to increasingly valuable personal data. Knowing people's preferences and purchasing habits was to revolutionize marketing industries – right down to targeting children (Steeves 2005).

A third phase of dataveillance only began to take off at the turn of the twenty-first century. It involves a device that had been in the analytical shadow of the internet during much of the 1990s but which, some argue, may be at least if not more profound in its social implications. The cell phone (or mobile phone) is the single most important item in what might be termed 'mobiveillance'. If dataveillance started in the world of places, such as supermarkets, police stations and offices, then the use of networked technologies such as the internet virtualized it, producing what might be called 'cyberveillance'. Surfing data became significant within the virtual travels of the internet user. The advent of mobile or 'm-commerce', in which the actual location of consumers becomes an important value-added aspect of personal data – using RFID, automated road tolling or other technologies as well as cell-phones -- brings the activity that characterized 'surfing' back into the world of place, only now it

can be any place in which signals are accessible (Andrejevic 2004, Lyon 2006).

The result is that personal data now circulate constantly, not only within but also between organizations and even countries. Personal data flow internationally for many reasons, in relation, for example, to police data-sharing arrangements (such as the Schengen Agreement in Europe), especially with the rise of perceived threats of terrorism, or to 'outsourcing,' the set of processes whereby banks, credit card companies and other corporations use call centres in distant countries for dealing with customer transaction data. While for much of the time publics in countries affected by such increased data flows seem to assume that their data are secure and that they are used only for the purposes for which they were released, notorious cases of fraud and sheer error do seem to proliferate with the result that some consumers and citizens are more cautious about how they permit their data to travel. The language used to mobilize such concerns is, more often than not, 'privacy'. Even if it is a notion of 'information privacy' rather than, say, a right to be 'left alone' that is in question, privacy dominates the discourse.

### **The end of privacy?**

From the late twentieth century a common response to the massive growth of surveillance systems in the global north has been to ask whether we are witnessing the 'end of privacy'. What is meant by this? On the one hand, as many socially critical authors assert, there are fewer and fewer 'places to hide'

(see, e.g. O'Harrow 2005) in the sense that some surveillance systems record, monitor or trace so many of our daily activities and behaviours that, it seems, nothing we do is exempt from observation. On the other, a different set of authors see the 'end of privacy' as something to celebrate, or at least not to lament. In the face of growing e-commerce and the consequent mass of personal data circulating, Scott McNealy, of Sun Microsystems, most famously declared, 'Privacy is dead. Get over it!'

It is important to note that privacy is a highly mutable concept, both historically and culturally relative. If privacy is dead, then it is a form of privacy – legal, relating to personal property, and particularly to the person as property – that is a relatively recent historical invention in the western world. At the same time, this western notion of privacy is simply not encountered in some South-East Asian and East countries. The Chinese have little sense of personal space as westerners understand it, and the Japanese have no word for privacy in their language (the one they use is imported from the west).

The best-known writer on privacy in a computer era is Alan Westin, whose classic book, *Privacy and Freedom* (Westin 1967) has inspired and informed numerous analysts and policy makers around the world. For him, privacy means that '...individuals, groups or institutions have the right to control, edit, manage and delete information about themselves and to decide when, how and to what extent that information is communicated to others.' However, although this definition seems to refer to more than the 'individual,' the onus of responsibility to 'do something' about the inappropriate use of personal (and

other) data is on data-subjects. That is, rather than focussing on the responsibilities of those who collect data in the first place, it is those who may have grievances who have rights to have those addressed.

This emphasis has been questioned, for example by Priscilla Regan (1995) who argues that privacy has intrinsic common, public and social value, and that that therefore not only may individuals have a right to seek protection from the effects of misused personal data, but also organizations that use such data have to give account. The huge increase in surveillance technologies, for instance in the workplace and in policing, underscores this point. Today, data are not only collected and retrieved, but analysed, searched, mined, recombined and traded, within and between organizations, in ways that make simple notions of privacy plain inadequate. Valerie Steeves maintains that while Westin started out (in the 1960s) with a broader definition of privacy, the overwhelmingly individualistic context of American business and government interests, in conjunction with pressure to adopt new technology 'solutions' has served to pare down privacy to its present narrow conception (Steeves 2005).

### **Surveillance as social sorting**

To argue that privacy may not have the power to confront contemporary surveillance in all its manifestations is one thing. To propose an alternative approach is another. For, as in the case of the Orwellian and the panoptic imagery for capturing what surveillance is about, the language of privacy has

popular cachet. It is difficult to explain why 'privacy' is not the (only) problem that surveillance poses (Stalder 2002) when this is so widely assumed by lawyers, politicians, mass media and western publics. The best way of deflecting attention from a singular focus on privacy, in my view, is to consider surveillance as 'social sorting.'

One might say that 'to classify is human' but in modern times classification became a major industry. From medicine to the military, classification is crucial. As Geoffery Bowker and Susan Star show, the quest for meaningful content produces a desire for classification, or 'sorting things out' (Bowker and Star 1999). Human judgements attend all classifications and, from our perspective, these are critical. Classification allows one to segregate undesirable elements (such as those susceptible to certain kinds of disease) but it is easy for this to spill over into negatively discriminatory behaviours. South Africa under apartheid had a strong population classification system but it served to exclude, on 'racial' criteria, black people from any meaningful access to opportunity structures. Classification may be innocent and humanly beneficial but it can also be the basis of injustice and inequity. The modern urge to classify found its ideal instrument in the computer.

One way of thinking about surveillance as social sorting is to recall that today's surveillance relies heavily on ICTs. Both security measures and marketing techniques exploit the interactivity of ICTs to identify and isolate groups and individuals of interest to the organizations concerned. By gathering data about people and their activities and movements and analysing

secondary data (by 'mining' other databases) obtained through networked technologies, marketers can plan and target their advertising and soliciting campaigns with increasingly great accuracy. Equally, security personnel use similar strategies to surveil 'suspects' who have been previously identified or who fit a particular profile in the hope of building a fuller picture of such persons, keeping tabs on their movements, and forestalling acts of violence or terror.

These actuarial plans for opportunity maximization (marketing strategies for widening the range of target groups for products and services) and for risk management (such as security strategies for widening the net of suspect populations) represent a new development in surveillance. Though they have a long history, they contrast with more conventional reactive methods of marketing or security delivery. They are future rather than past oriented, and are based on simulating and modelling situations that have yet to occur. They cannot operate without networked, searchable databases and their newness may be seen in the fact that unsuspecting persons who fit, say, an age profile, may be sent email messages promoting devices guaranteeing enhanced sexual performance and others, much less amusingly, who simply fit an ethnic or religious profile, may be watched, detained without explanation or worse by security forces.

The 'surveillant assemblage' works by social sorting. Abstract data of all kinds – video images, text files, biometric measures, genetic information and so on – are manipulated to produce profiles and risk categories within a fluid

network. Planning, prediction, pre-emption, permitting, all these and more goals are in mind as the assemblage is accessed and drawn upon. Social sorting is in a sense an ancient and perhaps inevitable human activity but today it has become routine, systematic and above all technically assisted or automated (and in some sense driven). The more new technologies are implicated, however, the more the criteria of sorting become opaque to the public. Who knows by what standards a credit was unexpectedly turned down or an innocent terrorist suspect was apprehended? Of course, the sorting may be innocent and above question – surveillance, after all, is always ambiguous – but it is also the case that social sorting has a direct effect, for good or ill, on life-chances (see Lace 2005:28-32 for consumer examples).

The main fears associated with automated social sorting, then, are that through relatively unaccountable means, large organizations make judgments that directly affect the lives of those whose data are processed by them. In the commercial sphere, such decisions are made in an actuarial fashion, based on calculations of risk, of which insurance assessments provide the best examples. Thus people may find themselves classified according to residential and socio-demographic criteria and paying premiums that bear little relation to other salient factors. Equally, customers are increasingly sorted into categories of worth to the corporation, according to which they can obtain benefits or are effectively excluded from participation in the marketplace. In law enforcement contexts, the actuarial approach is replicated; indeed, Feely and Simon warned in the mid 1990s that forms of ‘actuarial justice’ were becoming evident. The ‘new penology’, they argue, ‘is



concerned with techniques for identifying, managing and classifying groups sorted by levels of dangerousness' (Feely and Simon 1994: 180). Rather than using evidence of criminal behaviour, newer approaches intervene on the basis of risk assessment, a trend that has become even more marked after 9/11.

### **Surveillance society and safety state**

The growth of the surveillance dimension of modern states warrants special attention and one way of indicating this is to refer to current conditions of social life as living in a 'surveillance society'. This is no more meant to be sinister than it is to refer to everyday practices of extracting personal data in the supermarket – for example -- as 'surveillance.' It simply draws attention to a key feature of contemporary life which is both so routine and taken-for-granted that it seems unremarkable and yet simultaneously has such far-reaching consequences that it demands social scientific scrutiny.

At the same time, life in a surveillance society reflects in part some expanding dimensions of the nation-state. Whereas in the mid and later twentieth century it may have been true to say that several more liberal countries considered themselves to be 'welfare states' in the early twentieth century the designation 'safety state' began to be more plausible as an overall descriptor (Raab 2005). More and more, the criteria by which policies of many kinds are judged is not the positive benefit for all so much as the minimization of risk. New

technologies designed to reduce risk are central to the emerging quest for the 'safety state', and they all entail surveillance of one kind or another.

In their work on policing, Ericson and Haggerty show how new communication technologies make possible faster transmission and contribute to a shift from local spatial emphases to 'microcentres of inscription' such as computer terminals in police cars (1997: 431). Organizational hierarchies are challenged by the same trends, and at the same time more 'remote control' becomes possible. In combination, the new technologies enable faster surveillance of the population for risk management purposes (as well as making the police themselves more vulnerable to scrutiny). What they say about policing has a familiar ring in other sectors as well. Surveillance is vital to risk communication because it 'provides knowledge for the selection of thresholds that define acceptable risks and justify inclusion and exclusion.' Thus, they go on, 'coercive control gives way to contingent categorization' and everyone is 'assumed to be "guilty" until the risk communication system reveals otherwise...' (1997:449).

Such trends have become more widespread and controversial in the West since 9/11. Airport and border management systems are on heightened alert according to just the same kind of criteria. The same kinds of surveillance systems, now further bolstered by the adoption of 'new' biometrics technologies (distinguished from the 'old' not because they have transcended their often racist and colonial 'anthropometric' origins but rather by their extensive use of CITs), are used for making 'biographical' profiles of human

populations to determine whether or not they may travel, exchange large sums of money, or be employed within given companies. Hence the scandals, from a civil liberties perspective, of 'no-fly lists' based on ethnicity, religion, or country of origin, that can also easily include 'mistaken identities.' Hence too, the ironic exacerbation of risk (to travellers and citizens) from the increasing reliance on other agencies (such as airport) to whom tasks have been outsourced, especially in countries such as the USA.

It is also, at least in part, the role played by ICTs that makes it important to consider both 'surveillance society' and 'safety state' together. For the kinds of risk communication (that may also be read as 'opportunity calculation') carried out by firms in relation to customers, and providing detailed profiles, are also of interest to the nation state. Not only are the methods of assembling profiles based on similar algorithms, the actual data gathered and analysed by those firms is also of interest to law enforcement agencies, especially in the so-called 'war on terrorism.' Thus in 2006, for instance, Google refused to hand over its search records to the US Department of Justice (DoJ), citing the privacy of its users and the protection of its trade secrets. In this particular case, the DoJ claimed they wished to test the effectiveness of web-filtering software but many civil libertarians and privacy advocates saw it as the thin end of the wedge. Government could also use search records to obtain highly personal records, in the name of 'national security.'

Thus while it is worth examining both the development of the 'surveillance society' for its routine dependence on the garnering and processing of

personal data, and the 'safety state' for its use of surveillance for risk communication, it is also important to see that the two work in an increasingly symbiotic relation with each other. If present trends continue, this particular social-economic-political nexus will become more and more significant in coming decades.

### **Politics of personal data**

Surveillance studies, as this sub-field is increasingly known (see Lyon, forthcoming), has often focused on the large-scale systems, institutions and technologies that promote and produce surveillance. This can result in some rather negative and dystopian perspectives, however, that give the impression that ordinary people whose everyday activities are surveilled are simply pawns, ciphers in an increasingly global surveillance machine. Without suggesting that such views have no merit, or that the balance of power is not tipped overwhelmingly in favour of those large institutions, it is nevertheless important to note that surveillance is an interactive process. What sociologists of technology call 'co-construction' describes well the world of surveillance (Lyon, 2004).

In order to work, surveillance systems depend on their subjects (indeed, as Foucault observed a long time ago, subjects become 'the bearers of their own surveillance' 1979). Although there is a sense in which the subjects of surveillance become 'objectified' as their data doubles becomes more real to the surveillance system than the bodies and daily lives from which the data

have been drawn, their involvements with surveillance systems often remains active, conscious and intentional. People comply (but not as dupes), negotiate and at times resist the surveillance systems in which their lives are enmeshed.

It is very important to consider the ways in which so-called 'data subjects' of contemporary surveillance engage with and respond to having their data collected and used by organizations. Much depends on the purposes for which those data are collected. Righteous indignation at being shut out of a flight may be the response of a passenger with a 'suspicious' name, even though that same passenger may be delighted with the 'rewards' from his frequent flyer program with which he 'bought' the ticket. In each case, extensive personal data is used to determine the outcome, whether the privileged category of an 'elite' passenger or the excluded category of a name on the no-fly list. Consumers appear most willing to provide their personal data, in the belief that some benefit awaits them; employees and citizens are much more likely to exercise caution or express complaint at the over-zealous quest of organizations for their details.

Other variables in the analysis of the interactions between the 'watchers and the watched' include the extent of 'data subjects' knowledge of being watched. In the classic case of panoptic surveillance, prison inmates were supposed to subject themselves to self-discipline based on the assumption that the unseen inspector might just be watching. The uncertainty is essential to the success of the system. But what of situations where cameras are

hidden, or when customer details are simply extracted without the knowledge of the person concerned? Life-chances and choices are still affected, for better or for worse, but the opportunity to engage with the surveillance system is severely restricted. As ICTs help to reduce the visibility of surveillance through miniaturization or automation, this will become an increasingly significant area for social and political analysis.

The evidence suggests that the politics of information is becoming more important, even though some leading theorists of information may miss it. Manuel Castells, for instance, reassures his readers that for most of the time contemporary surveillance is a rather benign set of processes and Scott Lash argues that with the 'predominance of communication the logic of classification disappears' (2002:112). Yet as I have tried to show here, the use of ICTs within new regimes of risk management in the surveillance society and the safety state is contributing to new modes of classification that have profound social, economic and political ramifications. This is where the struggle over information will take place.

## **Conclusion**

Questions of surveillance and privacy have become more important as so-called information societies – dependent upon electronic technologies -- have developed since the 1970s. Thus ICTs are centrally implicated in these developments because their establishment may be prompted by them or they may be harnessed to add power to surveillance systems. At the same time,

surveillance grows because of certain economic and political priorities and because of the emergence of cultural contexts in which self-disclosure is not merely acceptable but sometimes positively valued and sought. Surveillance has also been expanding since the start of the twenty-first century in an international response to global terrorism, and it is now much more internationally networked itself, which again indicates how its dominant forms are structurally dependent on ICTs.

Calls for greater privacy, once the standard response to increased surveillance, continue to be made, with varying results. Yet regulative bodies, especially ones based on legislative regimes, have a very hard time keeping up with the changes occurring. At the same time, the onus of law has tended to be on the individual who feels (assuming she even knows) that she has been violated or invaded, and not necessarily on the organizations that process the data in the first place. Data protection regimes have more to offer here, dependent as they are on registering their activities, and more recent laws – for instance PIPEDA (Personal Information Protection and Electronic Documents Act 2001) in Canada – do require organizations, in this case including commercially based ones, to attend to the stipulations of the law.

But large and urgent questions about social sorting remain, even after privacy and data protection policies and laws have done their work. It is quite possible for negative discrimination to be carried out, automatically and systematically, against ethnic (such as categories relating to the likelihood of terrorist involvement) or social-economic (such as those living in low-income districts

of cities) minorities, despite having such policies and laws in place. The codes by which persons and groups are categorized are seldom under public scrutiny (and if they relate to 'national security' they may well be veiled in official secrecy) and yet they have huge potential and actual consequences for the life chances and the choices of ordinary citizens.

Thus both in terms of accurate analysis and informed political action, much remains to be done in the emerging realm of database-enabled surveillance. It seems unlikely that the issues will be tackled in ways appropriate to the present challenge while the mass media encourage complacency about self-disclosure, high technology companies persuade governments and corporations that they have surveillance 'solutions' to their problems, actuarial practices deriving from insurance and risk management dominate the discourse that support surveillance and legal regimes are couched in the language of supposed rights to individual privacy.

One upshot of this kind of argument is that analysts and practitioners in the ICT field have special responsibilities to understand and to intervene in an informed way in current developments. Beyond this, as I have argued, is an urgent need to go beyond tired notions of 'privacy' – that tends to place the onus of care with personal data back on the individual – to assessing the need for greater accountability in organizations processing personal data, as well as for greater awareness among publics, politicians and policy-makers. While common prudence may be expected, to assume that ordinary people have the time, expertise or motivation to be constantly vigilant about



surveillance is to sidestep questions of justice and informational fairness. The politics of information in the twenty-first century will increasingly be about how to increase the accountability of those who have responsibility for processing personal data.

## **Bibliography**

6, P. (2005), 'The Personal Information Economy: Trends and Prospects for Consumers', in S. Lace (ed.) *The Glass Consumer: Living in a Surveillance Society*, Bristol, UK: Policy Press, pp. 17-43.

Agamben, G. (1998), *Homo Sacer: Sovereign Power and Bare Life*, Stanford CA: Stanford University Press.

Andrejevic, M. (2004), *Reality TV: The Work of Being Watched*, New York: Rowman and Littlefield.

Bauman, Z. (2000), 'Social issues of law and order', *British Journal of Criminology*, 40:205-221.

Ball, K. and Webster, F. (eds. 2004), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, London: Pluto Press.

Bigo, D. and Guild, E. (ed. 2005), *Controlling Frontiers: Free Movement Into and Within Europe*, Aldershot UK: Ashgate.

Bowker, G. and Star, Susan. (1999), *Sorting things out: Classification and its consequences*, Cambridge MA: MIT Press.

Burrows, R. and Gane, N. (forthcoming), 'Geodemographics, software and class,' *Sociology*.

- Clarke, R. (1988), 'Information Technology and Dataveillance'.  
*Communications of the ACM*, 31(5), pp. 498-512.
- Cole, S. (2001), *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: Harvard University Press.
- Dandeker, C. (1990), *Surveillance Power and Modernity*, Cambridge: Polity Press.
- Deleuze, G. (1992), 'Postscript on the Societies of Control', *October*, 59, MIT Press, Cambridge, MA, pp. 3-7.
- Ericson, R. and Haggerty, K. (2000), 'The Surveillant Assemblage', *British Journal of Sociology*, 51(4), pp. 605-622.
- Ericson, R. and Haggerty, K. (1997), *Policing the Risk Society*, Toronto: University of Toronto Press.
- Feely M. and Simon, J. (1994), 'Actuarial Justice: The Emerging New Criminal Law', in D. Nelken (ed.) *The Futures of Criminology*, London: Sage, pp. 173-201.
- Flaherty, D. (1989), *Protecting Privacy in Surveillance Societies*, Chapel Hill: University of North Carolina Press.
- Foucault, M. (1979), *Discipline and Punish*, New York: Vintage.
- Gandy, O. and Deanna, A. (2001), 'All that glitters is not gold: Digging between the surface of data mining,' *Journal of Business Ethics*, 40, 373-386.
- Gandy, O. (1993), *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.
- Gandy, O. (1989), 'The Surveillance Society: Information Technology and Bureaucratic Social Control', *Journal of Communication*, 39(3), pp. 61-76.

Genosko, G. (forthcoming), 'Tense Theory' in D. Lyon (ed.) *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton UK: Willan Publishing.

Hardt, R. and Negri, A. (2000), *Empire*, Cambridge, MA: Harvard University Press.

Lace, S. (2005), *The Glass Consumer: Life in a Surveillance Society*, Bristol UK: The Policy Press.

Lash, S. (2002), *Critique of Information*. London: Sage.

Lessig, L. (1999), *Code and other laws of cyberspace*, New York: Basic Books.

Lyon, D. (forthcoming), *Introducing Surveillance Studies*, Cambridge: Polity Press.

Lyon, D. (forthcoming 2006), 'Why Where you are Matters: Mundane Mobilities, Transparent Technologies and Digital Discrimination', in T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York and London: Routledge.

Lyon, D. (2004), *ID Cards: Social Sorting by Database*, Oxford: Oxford Internet Institute Issue Brief  
([www.oii.ox.ac.uk/resources/publications/IB3all.pdf](http://www.oii.ox.ac.uk/resources/publications/IB3all.pdf))

Lyon, D. (2004), 'Surveillance Technology and Surveillance Society', in T. Misa, P. Brey, and A. Feenberg, (eds.) *Modernity and Technology*. Cambridge, MA: MIT Press, pp. 161-184.

Lyon, D. (ed. 2003), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London and New York: Routledge.

Lyon, D. (2003), *Surveillance after September 11*, Cambridge: Polity Press

- Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Oxford: Open University Press.
- Marx, G.T. (1998), 'Ethics for the new surveillance', *The Information Society*, 14:171-185.
- Marx, G.T. (1988), *Undercover: Police Surveillance in America*, Berkeley CA: University of California Press.
- Marx, G. T (1985), 'The Surveillance Society: the threat of 1984-style techniques', *The Futurist*, June: 21-26.
- McCahill, M. (2002), *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Cullompton: Willan.
- Norris, C. (2003), 'From Personal to Digital: CCTV, the Panopticon and the Technological Mediation of Suspicion and Social Control', in D. Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London and New York: Routledge, pp. 249-281.
- Norris, C. and Armstrong, G. (1999), *The Maximum Surveillance Society: The Rise of CCTV*, Oxford: Berg.
- Norris, C. and McCahill, M. (2004), *CCTV in London*, Berlin: Urban Eye ([www.urbaneye.net/results/ue\\_wp6.pdf](http://www.urbaneye.net/results/ue_wp6.pdf)).
- O'Harrow R. (2005), *No Place to Hide*, New York: Free Press.
- Raab, C. D. (2005), 'Governing the safety state', inaugural lecture at the University of Edinburgh, Scotland (June 7).
- Regan, P. (1995), *Legislating Privacy*, Chapel Hill: University of North Carolina.
- Rose, N. (1996), *Powers of Freedom*, Cambridge UK: Cambridge University Press.

- Rule, J. (1973), *Private Lives, Public Surveillance*, London: Allen Lane.
- Stalder F. (2002), 'Privacy is not the Antidote to Surveillance', *Surveillance and Society*, 1(1), pp. 120-124, Available: <http://www.surveillance-and-society.org/articles1/opinion.pdf>.
- Steeves, V. (forthcoming 2005), 'It's not Child's Play: The Online Invasion of Children's Privacy'. *University of Ottawa Law and Technology Journal*. 2 (2).
- Westin, A. (1967), *Privacy and Freedom*, New York: Atheneum.
- Winner, L. (1977), *Autonomous Technology: Technics out of control as a theme in human thought*, Cambridge MA: MIT Press.
- Wuthnow, R. (1998), *The Restructuring of American Religion*, Princeton, NJ: Princeton University Press.