The Electronic Eye
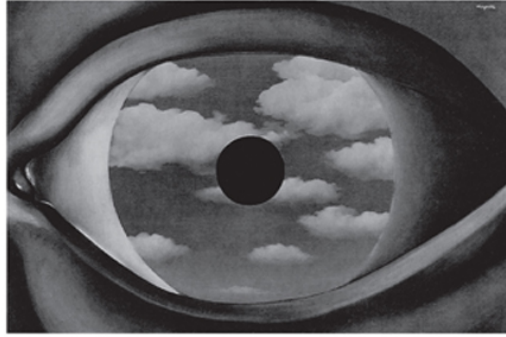
THE RISE OF SURVEILLANCE SOCIETY

DAVID LYON

The Electronic Eye

THE RISE OF SURVEILLANCE SOCIETY

DAVID LYON

The Electronic Eye

The Rise of Surveillance Society

DAVID LYON

Polity Press

Contents

Preface and Acknowledgements

Great excitement was generated during the 1970s and early 1980s about the arrival of new social conditions. Computer and communications technologies had made possible the 'Information Society'. All manner of benefits awaited us; new prosperity, new democratic and educational opportunities, a 'global village' thanks to new telecommunications, and a realignment of workplaces and class relations. There is no denying that advantages do indeed accrue from such technological development, but a little historical reflection and sociological imagination makes warning bells ring.

A number of writers - including me, in *The Information Society Issues and Illusions* - took it upon themselves to assess just what was going in the so-called information revolution. I argued that each situation should be analysed in its own right, that new technologies may well be implicated in some radical social changes that we don't yet understand fully, but that utopian dreams of wholesale societal megashifts were at best misleading hyperbole and at worst dangerous delusions.

Since then, the debates surrounding new technology have tended to become much more sober, if not sombre. The failure of computer-based service economies to lift the world out of recession, the advent of electronic war, and the dismayed realization that computers have a huge capacity to track the tiny details of our personal lives, have all helped foster more forbidding social forecasts. Even fearing the spectre of 'Big Brother' scarcely seems to do justice to the

new mood. The term 'surveillance society' was first coined in 1985; the warning note is growing in volume.

Of all the questions raised by new technologies, the one that strikes me as being most socially pervasive is the garnering of personal information to be stored, matched, retrieved, processed, marketed and circulated using powerful computer databases. The result of my investigation is this book, in which I examine the major dimensions of what we now speak of as 'surveillance'. Whereas once this had a fairly narrow meaning, to do with policing or espionage, surveillance is used here as a shorthand term to cover the many, and expanding, range of contexts within which personal data is collected by employment, commercial and administrative agencies, as well as in policing and security.

But I do not conclude that surveillance is solely sinister. Having tried earlier to puncture inflated optimism about the information society, I now try to soften the scaremongering alarms about surveillance society. Rather than view contemporary societies in which surveillance capacities are constantly augmented by computers merely as the sites of tighter social control, I suggest that surveillance often shows two faces. The processes that may seem to constrain us stimultaneously enable us to participate in society. We may be tracked by our Social Insurance Number, for instance, but the same computerized system ensures we receive unemployment benefits. The electronic eye may blink benignly.

The question then becomes more subtle. At what points, under what circumstances, and by what criteria is the current computer-aided surveillance undemocratic, coercive, impersonal or even inhuman? 'And when is it innocuous or a channel of positive blessing? Such questions must be addressed historically, sociologically, and politically. They involve normative judgements at every level. And they

entail engagement with present day debates about post-modernity, partly because new technologies are already implicated in those discussions and partly because conventional views of 'self or 'citizen' are disputed within them. My own route through these troubled waters, let it be said from the outset, is guided by converging traditions of Christian social thought. I may not see the Morning Star very clearly, but readers should at least know how I tried to set my course.

Part I

Situating Surveillance

1

Introduction: Body, Soul and Credit Card

'An individual in Russia was composed of three parts; a body, a soul and a passport.'

Vladimir Medem[1]

Surveillance in Everyday Life

This book, while it certainly doesn't ignore 'bodies and souls' is primarily about the 'passport' aspect of human existence. That is to say, I focus on that dimension of social life which today is vital to most relationships and transactions, apart from those of the most intimate or familial kind. Passports get us across borders, who drivers' licences are taken more seriously than our own word for proving who we are. In much of modern life we deal with relative strangers, and to demonstrate our identity or reliability we must produce documentary evidence. Indeed, the Russian proverb above should really be updated to

indicate that human beings would now be defined more accurately as 'body, soul and credit card'.

The other side of the coin, however, is that organizations of many kinds know us only as coded sequences of numbers and letters. This was once worked out on pieces of paper collated in folders and kept in filling cabinets, but now the same tasks - and many others, unimaginable to a Victorian clerk - are performed by computer. Precise details of our personal lives are collected, stored, retrieved and processed every day within huge computer databases belonging to big corporations and government departments. This is the 'surveillance society'.[2]

No one is spying on us, exactly, although for many people that is what it feels like if and when they find out just how detailed a picture of us is available. 'They' know things about us, but we often don't know what they know, why they know, or with whom else they might share their knowledge. What does this mean for our sense of identity, our life-chances, our human rights, our privacy? What are the implications for political power, social control, freedom and democracy? This book addresses just such questions.

In one, limited, sense the electronic component of surveillance is nothing new. Wiretapping and other forms of message interception have been the common currency of espionage and intelligence services for many decades. But what this book explores is how, to an unprecedented extent, ordinary people now find themselves 'under surveillance' in the routines of everyday life. In numerous ways what was once thought of as the exception has become the rule, as highly specialized agencies use increasingly sophisticated means of routinely collecting personal data, making us all targets of monitoring, and possibly objects of suspicion.

Surveillance, as described here, concerns the mundane, ordinary, taken-for-granted world of getting money from a bank machine, making a phone call, applying for sickness

benefits, driving a car, using a credit card, receiving junk mail, picking up books from the library, or crossing a border on trips abroad. In each case mentioned, computers record our transactions, check against other known details, ensure that we and not others are billed or paid, store bits of our biographies, or assess our financial, legal or national standing. Each time we do one of these things we actually or potentially leave a trace of our doings. Computers and their associated communications systems now mediate all these kinds of relationships; to participate in modern society is to be under electronic surveillance.

All this did not develop overnight, and indeed part of what we must examine is the relatively long history of the 'surveillance society.' Today's situation cannot be understood without reference to the long-term historical context. Ever since modern governments started to register births, marriages and deaths, and ever since modern businesses began to monitor work and keep accurate records of employees' pay and progress, surveillance has been expanding. Surveillance denotes what is happening as today's bureaucratic organizations try to keep track of increasingly complex information on a variety of populations and groups. Yet it is more than just 'bureaucracy.' Surveillance is strongly bound up with our compliance with the current social order, and it can be a means of social control.

At the same time, surveillance systems are meant to ensure that we are paid correctly or receive appropriate welfare benefits, that terrorism and drug-trafficking are contained, that we are made aware of the latest consumer products available, that we can be warned about risks to our health, that we can vote in elections, that we can pay for goods and sevices with plastic cards rather than with the more cumbersome cash, and so on. Most people in modern societies regard these accomplishments as contributing

positively to the quality of life. So surveillance is not unambiguously good or bad; and hence the dilemmas surrounding the use of computer databases for storing and processing personal data.

Surveillance expands in subtle ways, often as the result of decisions and processes intended to pursue goals such as efficiency or productivity. Moreover, its subtlety is increased by its present-day electronic character. Most surveillance occurs literally out of sight, in the realm of digital signals. And it happens, as we have already seen, not in clandestine, conspiratorial fashion, but in the commonplace transactions of shopping, voting, phoning, driving and working. This means that people seldom know that they are subjects of surveillance, or, if they do know, they are unaware how comprehensive others' knowledge of them actually is.

Though modern surveillance originated in specific institutions such as the army, the corporation, and the govenment department, it has grown to touch all areas of life. This was brought home to me personally during a recent move from Britain to Canada. My family and I could not fully participate in Canadian society until our details had been transferred into a number of electronic databases. This began on arrival at Toronto International Airport, as the travel-tired family lined up at Employment and Immigration Control. Details had to keyed into the computer before we could continue to our destination in Kingston, Ontario.

No sooner were we installed in Kingston than we had to obtain health care cards, Social Insurance Numbers, bank cards and a university staff card, each of which relates to personal details stored in a compouter database. We could not be employed, acquire medical or accident coverage, or obtain money without these. However much we like cycling, it is hard to get around without a car, so we had to get drivers' licences, which again link our records by computer. Surprisingly soon after arriving, we started receiving

'personal' advertising mail which indicated once more that yet other computers contained data about us, gleaned from the telephone company, which also lists - and sells - essential facts about us. Other agencies than the phone company do just the same.

As soon as we began the process of buying a house, the quest for electronic verification intensified. Mortgage companies demanded details of the crucial Social Insurance Number (which would reveal immediately whether we were *bona fide* citizens, permanent residents or temporary workers) because such financial transactions are of interest to the tax authorities. Equipping ourselves with a cooking stove, washing machine and fridge involved similar proof of (credit-) worthiness in terms of bankcard and credit-card numbers. As a university professor, I find myself in the relatively privileged position of either possessing the right number sequences to unlock these electronic doors or of being able to explain that things will soon be in place. But the same processes are clearly experienced in quite different ways by those lacking access to the appropriate plastic cards or numbers.

In other words, participating in just about every aspect of modern life depends upon our relationship with computer databases; and to process our personal details we rely not only upon professional experts and bureaucratic systems, which have increasingly become a feature of modern life in the twentieth century, but upon electronic storage and communication devices. What difference, if any, does this make to social, political and cultural life? The answer to this crucial question draws us into a number of important debates, sometimes in disciplinary areas that are conventionally separate. I shall list these below, but thoughout the book I shall show how they must be considered together if we are properly to grasp the dimensions and implications of the 'surveillance society.'

The genius, and the usefulness, of sociology lies in locating particular events and trends in their broader structural and historical context. In this way we can begin to distinguish between the short-term aberration from some norm and the long-term break with existing conditions, between the socially significant and the trivial or the transient. This book aspires to place elctronic surveillance - in a broad sense, rather than the narrower 'security-and-intelligence' sense - in just such a social and historical context, and to show where it came from, what - if anything - is new about it, what are its future prospects and wider implications, and what might seem to be appropriate responses to its development. This should become clear as we consider the various debates within which electronic surveillance is properly situated.

Surveillance in Modern Society

Until a decade ago, surveillance occupied no distinct place in the sociological lexicon. Despite the fact that James Rule's groundbreaking study of *Private Lives and Public Surveillance* had appeared in the early 1970s, quickly establishing itself as the standard text,[3] it was not until Michel Foucault's celebrated, and contentious, historical studies of surveillance and discipline had appeared that mainstream social theorists began to take surveillance seriously in its own right. Surveillance, insisted Anthony Giddens[4] and others, should be viewed not merely as a sort of reflex of capitalism (monitoring workers in the factory), or of the nation-state (keeping administrative tabs on citizens), but as a power-generator in itself.

Of course, we can now look back at many other sociological studies and see how they concerned processes very closely related to what today we call surveillance. Prominent here is work carried out in two major traditions,

the Marxian and the Weberian. Karl Marx focuses special attention on surveillance as an aspect of the struggle between labour and capital. Overseeing and monitoring workers is viewed here as a means of maintaining managerial control on behalf of capital. Max Weber, on the other hand, concentrates on the ways that all modern organizations develop means of storing and retrieving data in the form of files as part of the quest of efficient practice within bureaucracy. Such files frequently contain personal information so that organizations, especially government administrators, can 'keep tabs' on populations.

Foucault's more recent contribution to surveillance theory, though sophisticated, may be simply stated. Modern societies have developed rational means of ordering society that effectively dispense with traditional methods like brutal public punishment. Rather than relying on external controls and constraints, modern social institutions employ a range of disciplinary practices which ensure that life continues in a regularized, patterned way. From army drill to school uniforms, and from social welfare casework to the closely-scrutinized factory worker's task, the processes of modern social discipline are depicted in sharp relief. Others have taken his analysis beyond the spheres he considered, for instance into the ways women are disciplined to dress and present themselves as 'feminine' in male-dominated society.[5] Furthermore, as these examples imply, people co-operate and collude with the means of control.

Specialized knowledge strengthens the power of each modern agency, and taken together they seem to colonize ever-increasing tracts of so-called private life. The categories and classifications imposed, whether they be the time for performing a work-task or raising a rifle or the calculation of health or crime risk, induce, according to Foucault, progressively sharper distinctions between acceptable and unacceptable behaviour. This in turn defines

the 'normal' human individual, thus creating what we think of as social order. In this way people are produced as subjects - or, more accurately, objects.

Foucault's role in surveillance studies is curious and paradoxical. With careful empirical studies of surveillance, such as Rule's, available, it yet took someone who was notorious for his disdain of data to set the debate fully in motion. One of the oddest things about Foucault is his silence about that acme of rational classification, the computer. Surely, if anything accelerates the process of monitoring the routines of everyday and producing people as objects it is the computer! But the task of applying Foucault's analysis to the social role of information technology - and quite an array of plausible interpretations is available! - has been left to others. The apparent relevance of Foucault's analysis may be obvious, but the way that some of the connections have been made actually arouse further controversy.

For one thing, many commentators have lighted eagerly upon Foucault's image of the Panopticon prison plan[6] as an examplar of electronic surveillance. Some apply it only to specific social milieux, such as industrial organizations, while others glimpse here the contours of a completely new social formation, comparable to Marx's depiction of the 'mode of production'. At one extreme this can be taken to mean that wherever computer databases process human data we are caught up in some system of total, prisonlike domination, which seems to me to be nonsense. However, even milder versions of this idea rightly raise the question of resistance; what can be done in the face of such all-encompassing power? This is what this book tries to explore.

The idea of the 'surveillance society' is used to capture this particular dimension of modern social life.[7] The perspective outlined in this book takes account of what Marx, Weber and Foucault have to say, but is not exclusively

aligned with any one of them. In any case, the sociological debate has been joined by others, notably Anthony Giddens, who locate the processes of surveillance within modern society as one of its major isntitutional dimensions. His work is a useful springboard[8] for surveillance studies, but, as we shall see, it too invites modification, particularly in the light of the electronic character of surveillance.

In the sections that follow I indicate the kinds of debates within which surveillance features. These debates overlap, and greater integration between them could only be beneficial. The order in which they are listed implies no priority.

The Social Impact of Technology

Electronic surveillance has to do with the ways that computer databases are used to store and process personal information on different kinds of populations. Examining the 'surveillance society' may be seen as a case study in the interaction between technology and society. I say 'interaction' advisedly, because there are several stances on the society/technology relationship.

Some writers place the emphasis on the ways that new technologies determine the direction of social development. This impression could be given, for instance, by titles such as Alvin Toffler's *The Third Wave*,[9] which seem to imply that social change is technology-driven. Both extreme optimists and extreme pessimists on the question of the social role of technology are prone to this error, which is known as technological determinism. It underestimates both the role of social factors in shaping the technology in the first place, and also the variety of social contexts that mediate its use.

Other commentators put such stress on the social relations expressed in the technologies that they seem to have little time for considering how specific technologies

might have intrinsic constraining or enabling consequent for social relations. Some Marxists succumb to this temptation, following Marx's gloss that machinery is 'a power inimical [to the worker] and as such capital proclaims it from the rooftops and as such makes use of it'.[10] In the laudable attempt to uncover the social relations obscured by apprently asocial machines like computers, they sometimes seem to deny that the artifact itself could have some consequences that are intrinsic to it.[11]

Electronic surveillance, I argue, is both socially shaped and has social impacts, but the nature of the shaping does not necessarily render the impacts predictable in any straightforward sense. Certain capacities of the technological systems themselves make them attractive for use in ways hitherto unimagined. This kind of approach comports well with Gary T. Marx's studies of what he calls the 'new surveillance'. In the course of a major analysis of undercover police work in the USA, he found that the use of computer technologies does indeed make a difference, for a number of important reasons.[12]

Computer matching provides a good example of this relatively independent characteristic of new technology. The power of computer systems to relate data from various sources and gathered with different purposes has inspired numerous experiments with personal information. Two or more unrelated computerized files of individuals are matched to identify groups of people in a similar category, such as suspected law-breakers. Computer matching is a technique used first by government departments in the late 1970s, and it was widespread by the early 1990s. Quite *how* widespread is not always known exactly. During 1991, for instance, the Ontario Information and Privacy Commission proposed that a task force be established to discover just how extensive computer matching is within and between different departments of the provincial government.[13] In

Australia, especially since 1987, computer matching has grown apace, so that by October 1990 there were thirty-one active and proposed major data-matching programmes involving government departments.[14]

In the USA, the technique began in 1977, when the then Department of Health, Education and Welfare matched welfare files of federal government departments in what turned out to be a somewhat abortive attempt to expose fraud.[15] To illustrate its potential in other areas, a bizarre case concerns an America business, Farrell's Ice Cream Parlour, which sold the name-list of those claiming free sundaes on their birthdays to a marketing firm. Soon after, the ice-cream eaters were surprised to find draft registration warnings in their mail! The marketing company had sold their details to Selective Service System, who had in turn sold them to the Department of Defence.

More routinely, employee records of the American Civil Service Commission have been matched with those of family welfare recipients in order to root out fraud, and, at the other end of the social spectrum, the Department of Heath and Human Services matches relevant files to check that no doctors are double-billing the health insurance schemes of Medicare and Medicaid.[16] Comparing files on such a huge scale is clearly only possible using computers so, such investigations are technologically facilitated. But once begun, computer matching has huge implications. Anyone can be caught in the computer dragnet, and may be presumed guilty until proven innocent. Existing privacy laws have been powerless in this respect.

It is this kind of realization that lends weight to the view that such computer systems grow 'out of control'. David Burnham's fascinating -and frightening - book, *The Rise of the Computer State*,[17] for instance, implies that new computer technologies augment themselves beyond the direct control of anyone, let alone elected decision-makers.

At odds with this 'autonomous technology' position, however, are observers who see new technology almost as a tool of capitalism or of repressive states. Kevin Wilson's *Technologies of Control*,[18] for example, portrays the home networking of computers as 'data-based social control'. Here, computer-power appears to be used deliberately as a means of obtaining compliance.

The stance taken in the following pages is that while new technologies do indeed have a kind of self-augmenting capacity (the phrase, by the way, is Jacques Ellul's)[19] this does not make them immune from sociological scrutiny. The process by which they are augmented is all-too-often a 'black box'. We should open the box and analyse the contents; we may well discover some deeply social factors shaping the technologies. At the same time, I do not wish to underestimate the extent to which new technologies may contribute to the processes of social control. But the story is a subtle one, and cannot be reduced to any crude categories that assume that surveillance is born of a malign collusion of economic and political power.

One interesting challenge to surveillance studies presented by processes such as computer-matching is that an essentially technical procedure may contribute to the blurring of conventionally conceived boundaries. Anthony Giddens, for instance, distinguishes between surveillance as 'gathering data on' and 'supervising' people.[20] But this may be less salient as forms of 'supervision' by various agencies - including employers, who might once have monitored their workers in a more direct manner - are actually achieved by 'data gathering'.

These then are the general contours of the technology-and-society debate within which electronic surveillance may be situated. The niceties of debate must not, however, be allowed to obscure the significance of the particular case considered here. Our topic represents the single most

controversial and potentially alarming social issue prompted by the massive expansion of computer power in human affairs. Modern society makes us all radically dependent upon the realm of expert knowledge, on people 'in the know'. The key question addressed here is, what difference for good or ill does it make to mediate that knowledge through powerful computer systems?

Technology and Totalitarianism

The vexed question of computers, power and domination conjures up a variety of sinister images. The best know of these is Orwell's dystopia, *Nineteen Eighty-Four*, where telescreens constantly monitor all activities. The nation-state now comes into the foreground, and with it the commonplace post-war contrast between totalitarianism and democracy. If Giddens is right to say that 'Totalitarianism is, first of all, an extreme focusing of surveillance'[21] then the enhanced role of new technology within government administration and policing should give us pause.

It is important to note that the influence of Orwell's *Nineteen-Eighty-Four* has been felt far beyond the merely literary. The metaphor of 'Big Brother', in particular, now expresses a profound cultural fear in areas quite remote from what Orwell originally had in mind. The impact of Orwell's dystopia has also been sociologically significant. James Rule explicitly refers to *Nineteen Eighty-Four* as the situation of 'total surveillance' from which he derives the concept of 'surveillance capacitie'.[22] Others, such as Christopher Dandeker in *Surveillance, Power and Modernity*,[23] carry the same concepts into sociological analysis of the 1990s.

The fact that the advanced societies are falling over themselves to adapt and upgrade their computing

capacities does not on itself mean that they are sliding down a slope into tyranny, However, if intensifying surveillance is a crucial component of totalitarianism, democratically-minded citizens would be justified in at least asking questions about the role of new technologies in government. After all, was it not in a highly civilized, rational, bureaucratic society that the techniques of the Holocaust were conceived and executed? As Zygmunt Bauman reminds us, moral standards are easily rendered 'irrelevant' to the technical success of bureaucratic operations. The objects of bureaucratic operation - people - are easily dehumanized.[24]

Over the past decade Social Insurance Numbers have been used for more and more purposes in Cananda, machine-readable passports have been introduced in Germany, electronic identity card systems have been proposed in Britain and Australia, and the driver's licence has become a *de facto* personal identifier in the USA. Yet such developments occur all too often without extensive public discussion and policy debate. Sir Norman Lindop, chairman of the British Data Protection Committee, reporting as early as 1978, commented that

> We did not fear that Orwell's *1984* was just around the corner, but we did feel that some pretty frightening developments could come about quite quickly and without most people being aware of what was happening.[25]

As we shall see, just what Lindop feared has occurred, and not only Britain.

Other problems also exist besides bureaucratic momentum and public ignorance. One is that personal databases proliferate in areas which are not directly within the ambit of administration and policing but which, given the increasing ease of communications between computers, may interact with them. This happens by all manner of routes, including the leakage of public sector data to the

private sector *via*, for example, insurance companies, private policing (whose findings are used by statutory police forces), and the monitoring of exmployees; this last has generated data used extensively within and outside government administration in vetting applicants for posts or promotion. In addition, being accepted as a fully participating member of society today depends more and more on one's ability to consume, and much contemporary surveillance is in fact commercial. How far are ordinary people's life-chances circumscribed or enhanced by such processes? Surveillance, which was once thought of as touching only the realm of political citizenship, now affects our involvement in society at a more basic level.

A further issue of note is the relative lack of countervailing organizations committed to investigating, and if necessary resisting, the spread of electronic surveillance. Other modern institutions seem to have provoked the forming of social movements that call them in question; capitalistic organization has been accompanied by the rise of labour movements, industrial expansion by Green movements, and so on. But to which groups or coalitions could one realistically turn for a critique of or reasoned opposition to electronic surveillance? Granted, civil liberties associations, consumer councils and some labour unions do play an active part in trying to contain or democratically channel its growth. But one doesn't have to be a pessimist to note the relative lack of such resistance.

On the positive side, we should note that there are some strong hints of a growing realization of the importance of surveillance issues. A casual review of popular media shows more frequent treatment of 'computer and privacy' issues, and during 1992 an important step was taken with the founding of Privacy International. This new organization exists to draw together data on surveillance data protection from widely scattered countries across the world.[26] From the

point of view of those concerned about surveillance this is a welcome move, especially as surveillance is an increasingly global phenomenon. The long-term impact of such attention and activity remains, however, to be seen.

I have already alluded to one reason for the relative lack of public resistance to contemporary surveillance. That is, many of its achievements are viewed - rightly - as positive social benefits. Why resist systems whose advantages simply carry with them a number of acceptable risks?

Another reason is no doubt the feeling that statutory agencies already take care of such matters. Data protection agencies, such as the Canadian Information Commission or the French Commission Nationale de l'Informatique et des Libertés (CNIL) have for some time acted as watchdogs or whistleblowers in their respective countries. Data protection and privacy legislation certainly offers some established limits to the unhindered growth of electronic surveillance, but, given the rate of technological change facilitating the processes mentioned above, such legal measures tend to lag behind to a significant and perhaps dangerous degree.

Added to this is another serious difficulty; lack of agreement on exactly what is the perceived problem. All too often the stock response to issues of surveillance is couched in the language of 'privacy'. Indeed, in North America the relevant legislation is normally termed 'The Privacy Acts'. The chief difficulty here is that the concept of privacy is stretched beyond its (socio)logical limits. Anxiety about totalitarian tendencies is inappropriately addressed under the 'privacy' rubric, though that may be one concern among others; 'Liberty' might make a preferable candidate. Equally, the possible limits on autonomy within the marketplace, imposed by commercial surveillance, are hardly confronted head-on when 'privacy' is brandished in resistance.

At the same time, simply abandoning privacy is as misguided a response as adopting it in an omnibus fashion. Neglecting the issue of privacy is to ignore some of the most profound challenges of the growth of electronic surveillance, even though that issue cannot properly cover some of the most significant issues raised by it.

The Problem of Privacy

Privacy was first mooted as a serious question for legal consideration during the last century. Expressed classically in the USA by Samuel Warren and Louis Brandeis, privacy is 'the individual's right to be left alone'. Although in 1928 Brandeis warned, ominously, that 'The progress of science in furnishing the Government with the means of espionage is not likely to stop with wiretapping', little did he guess just how far even 'the most intimate occurences of the home'[27] would become potentially transparent to a range of agencies courtesy of computer-power.

By 1948 - the year the transistor was invented - the United Nations declared as a human right that 'no one shall be subject to arbitrary interfence in his privacy, home or correspondence'. The word 'arbitrary' was clearly intended to contrast with, say, 'lawful', but who is to say what should be thus exempted? Or, for the matter, what exactly constitutes 'interference'? Thirty years later, when the microchip made its first appearance, such questions seemed even further from resolution. By then, governments and other large organizations were already making extenisive use of computer power to store and process personal data, and the more precise term 'information privacy' was proposed as a means of coping with the consequent broadening of perceived threats to privacy.

But what exactly is threatened by the rapid rise of computerized record-keeping, either by state or economic