The Electronic Eye

The Rise of Surveillance Society

DAVID LYON

University of Minnesota Press
Minneapolis

First published in 1994 by Polity Press
in association with Blackwell Publishers

First published in 1994 in the United States by
University of Minnesota Press
2037 University Avenue Southeast
Minneapolis, MN 55455–3092

Library of Congress Cataloging-in-Publication Data

Lyon, David, 1948–
The electronic eye : the rise of surveillance society / David Lyon.
p. cm.
Includes bibliographical references and index.
ISBN 0–8166–2513–1 (hc) 0–8166–2515–8 (pb)
1. Electronic surveillance—Social aspects. 2. Computers and civilization. 3. Information technology—Social aspects.
I. Title.
TK7882.E2L96 1994
303.48'33—dc20 93–35598
CIP

The University of Minnesota is an
equal-opportunity educator and employer.

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, prison-like 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 capacities'.[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 institutions? In Victorian times, the fear was that members of the public might obtain unseemly access to the private lives of élite people, such as politicians or the rich. British Royalty, among others, continue to struggle with this. With electronic surveillance, however, the equation is reversed. It is the lives of ordinary citizens that are thought to be at risk from large and powerful agencies. Indeed, the practice of computer-matching, mentioned earlier, tends to place the poor, the vulnerable, the minority at a particular disadvantage relative to big bureaucratic forces.

Unfortunately, and with a few important exceptions. sociologists have not given extensive attention to the debate over privacy and data protection. Until recently, many sociologists seem to have so preoccupied with opposing privat*ism* and familial*ism* that matters of human dignity, self-identity and personal space have fallen into neglect or left by default to other disciplines. Over recent decades the discourse on privacy has been dominated by legal opinion. Consequently, while some useful work has been done in an attempt to define privacy for the so-called information age, legal writers and philosophers have had to fall back upon what one of them, Geoffrey Brown, calls 'crude and homespun sociology'.[28]

The danger of such a relative lack of sociological analysis and discussion is that legal conceptions of privacy lose touch with technological and social realities.[29] Sociological and historical investigation highlight the cultural variations in privacy, and can show both what people actually fear and how well-grounded those fear are. Considerable headway has been made in this regard in the comparative studies produced by Canadian historian David Flaherty.[30] His work also addresses the key question of what social, political and economic difference is made by the advent of electronic surveillance. Beyond this, sociology may well play a part in uncovering and evaluating perceived threats to human liberty or privacy produced by apparently innocuous practices such as the management of consumer demand.

North American data protection laws, for example, tend to cover only government databanks, leaving huge swathes of commercial surveillance almost untouched. Thus when in 1991 Lotus advertized new business software on CD–ROM disks that reveal at the push of a button the names, addresses, marital status and estimated income of eighty million American householders, no law stood in its way. Indeed, the software had been approved for distribution by an experienced American privacy advocate, Alan Westin. Even before it was formally launched, however, Lotus received so many complaints that they withdrew the product. The incident indicates not only the weakness of legislation but also the paucity of privacy as an organizing concept. In an information technology environment such concepts requir overhauling.

Ironically, one of sociology's central themes since it began to define the parameters of modernity is precisely the relation of the so-called 'private' to the 'public' sphere. This debate – particularly as precipitated by feminist critique – is of immense importance to matters considered here under the rubric of electronic surveillance. The public/private dichotomy originates in classic liberalism. The former refers to the realm of politics and the state, which acts as an umpire, enforcing public laws. The latter includes the domestic realm, but can also refer to private interests, private enterprise

and private individuals. Sociologically, this is connected with the way that industrial production increasingly sent men 'out' to work and relegated women to the 'home'.

From the feminist critique it is plain that notions of public and private have been used to throw a veil over conflicts, struggles and abuse that occur all-too-often within the so-called private sphere. Thus the distinction carries heavy ideological freight. Dilemmas abound here too. Historical research shows that many women welcomed intervention in abusive situations.[31] Today, telephones with 'caller ID' facilities that display the caller's number to the called household are similarly welcomed by women in danger. The problem is that the same system, used in reverse, is a gold mine of consumer data for companies wishing to target specific buying groups. Our 'phones may reveal more than we wish to disclose!

During the 1990s, new telephone services promise to offer a major challenge to conventional concepts of privacy, particularly as far as this term applies to the domestic sphere, the 'home'. Caller ID is just one of them, but this has already generated considerable controversy in the countries where it is available.[32] While the telephone companies sell the services as a means of gaining control over what communications *enter* the home, marketers rub their hands with delight at their new corner on data *leaving* the home by the selfsame channel. It is indeed a Janus-faced technology, but one prominent critic, Marc Rotenberg, warns of a coming showdown as members of the public become aware that caller ID is a means of obtaining personal information without consent. 'From Ma Bell to Big Brother' is his slogan for it.[33] The once 'private' home is made 'public' means of convenient communications systems purchased by its residents.[34]

If it was ever appropriate analytically to separate 'public' and 'private' spheres, it certainly is not in then late twentieth century, when the boundaries between them have been thoroughly obscured. Indeed, to return to our central theme, information technology now enables further blurring of the boundaries, on a massive scale. The home, once a sacrosanct liberal haven from 'public' life, increasingly finds itself to be the site of surveillance. Government administration gains easy access to details of who lives with whom, and this affects voting capacity or welfare entitlements, while commercial agencies encounter few obstacles to analysing the financial standing and consumer preferences of each household in a given street.

All this throws into radical doubt the usefulness of 'privacy' as a concept that can cope sociologically (let alone legislatively!) with the challenge of electronic surveillance. At the same time, it would be premature to jettison any and all appeals to privacy, or to a 'personal' realm. The personal is

indeed political and power relations are evident in the public/private distinction. But one can still argue for a personal dimension to social life.[35] The nature of that 'personal' sphere constitutes another area of debate into which questions of electronic surveillance propel us.

Clearly, new dialogue is urgently needed between social scientists, legal thinkers and policy-makers if today's challenges to taken-for-granted assumptions about privacy and its security are to be contained or neutralized. Needless to say, such a dialogue would in part be contingent upon the willingness of sociologists to have an 'applied' role; and this in turn requires some redefinition.[36]

Personhood and Postmodernity

Lastly but by no means least, electronic surveillance must be situated within a cluster of problems that, for want of a better term, I have labelled 'personhood and postmodernity'. Personhood has to do with human identity, dignity, liberty and responsibility, which in different ways are assumed to be challenged by the rise of electronic surveillance, and in terms of which rules regulating its spread are framed. 'Postmodernity' refers to a debate about a social transformation supposedly taking place towards the end of this century, in which we move beyond the modern condition. I have placed personhood and postmodernity together to indicate that the study of electronic surveillance raises some fundamental philosophical questions that sociology *per se* cannot resolve but without attention to which sociology cannot proceed.[37]

A paradox lurks here. The impact of information technology in human affairs is sometimes taken to be one indicator that we are entering a qualitatively different phase of social development from that known as 'modernity'. Among other things, in the condtion of postmodernity it is sometimes said that we can no longer be as sure as we were of the status of human presonhood – apart from its being culturally and historically relatives. At the same time, the growth of electronic surveillance has thrown up questions about 'privacy' that ultimately can only be addressed in terms of some conception of personhood and human identity. Can those involved in the critique of electronic surveillance, the framing of law, and the establishment of policy, agree enough on what is important to construct appropriate measures relating to it? A couple of examples will give a flavour of the problem.

In *The Postmodern Condition*[38] Jean-François Lyotard paints a picture of society that is heavily dependent upon new information technologies. He follows Daniel Bell's[39] assertion that 'knowledge' has emerged as a new

axial principle of contemporary societies, and that new means of information processing are deeply implicated in this development. At the same time, this 'postmodern condition' is characterized by the 'collapse of metanarratives'. That is to say, modern verities such as the redemptive belief in science, technology or democracy, having fallen into some disrepute during the twentieth century, have now lost whatever universal power they might once have been thought to posssess. Lyotard asserts not only that they have collapsed, but that in a quest for some kind of certainty people clutch at the apparently certain methods of computer science as a substitute.

Information technology, in this account, stands in an ambiguous relation to postmodernity, part problem, part remedy. People trust themselves to complex technologies because they seem to promise convenience, efficiency, security and reduced uncertainty. Simultaneously, we worry that in so doing we may be denying something important to a worthwhile human life. But what that 'something' is becomes increasingly hard to define. We end, Lyotard might conclude, by depending on the very systems about whose efficacy we entertain nagging doubts. We collude with surveillance systems, whether willingly or reluctantly, wittingly or unwittingly. But if we object, we are unsure of our grounds for so doing.

Similar themes are taken up by Mark Poster, who argues persuasively that the postmodern could be classified as a 'mode of information'.[40] He too places the development of information technology – and particularly what we shall refer to as its surveillance capacity – at the centre of contemporary social transformation. He asks, for instance, where the human self is located if fragments of personal data constantly circulate withing computer systems, beyond any agent's personal control?

For Poster, the language of 'privacy invasion' is irrelevant, a throwback to modernity. In today's databases we see 'the constitution of an additional self, one that may be acted upon to the detriment of the 'real' self without that 'real' self ever being aware of what is happening'.[41] So what exactly is the status of our 'electronic image'?[42] And how does it affect or even connect with our other, more familar relationships in everyday life? And if we query the desirability of this 'virtual world', is it enough to counter it with a 'freedom of information' strategy, as Poster seems to advocate?

Both of these accounts present us with an intriguing and important challenge. Should current trends in the processing of personal data be interpreted as simply more of the same, and thus amenable to the kinds of analysis that began with Max Weber's studies of rationalization and bureaucracy? Or should they be considered as significant aspects of a deeper social transformation that requires the entire recalibration of

sociological concepts? Is the kind of surveillance that characterized the growth of modernity being supplanted by a new, postmodern surveillance, or is it merely the old surveillance writ large? Either way, the issues of what constitutes human personhood and of how that fits with conceptions of social order cannot be evaded.

Although these issues are addressed later in the book, a word on my own stance may be appropriate here. While I regard some from of surveillance as an inherent – and not necessarily evil – feature of all human societies, it seems to me that the chronic quest for personal data-collection that typifies modern life demands specific and urgent critical attention. Questions of justice and fairness must be raised when people's everyday activities are monitored and their habits, commitments and preferences classified by the would-be omniscient organization. Such classification is both an outcome not only of social differences but of advantage and disadvantage, and often serves to reinforce inequalities of life-chances. And while it undoubtedly enables us to participate in society in numerous important ways, it also constrains us and encourages us to comply with the social order. The more marginal or nonconforming we are, the stronger the web of constraint-by-surveillance becomes.

Surveillance is thus a morally and politically loaded activity, amenable to critique and to challenge; and not only from the macro-level political point of view. Issues of social inequality and social control are also connected with issues of trust and personal integrity. Particular forms of communication are a vital aspect of what it means to be human. What we disclose to whom, and under what conditions, is highly significant. What once we might have revealed, consciously, about ourselves to someone we trust – friend, doctor, priest, therapist – may now be involuntarily disclosed by electronic means to organizations or machines that we cannot know, let alone trust, in the same way. Our identity is understood by others – and by inanimate machines – more from our data-image than from our personal communication.

In other words, living in 'surveillance societies' may throw up challenges of a fundamental – ontological – kind. Not surveillance as such, but the specific surveillance trends of the late twentieth century seem to raise questions for which as yet we have far from adequate answers. While it would be foolish to imagine that this book would provide such 'answers; I hope that at least the questions will be made clearer. My own stance, which guides my choice between both theoretical and practical alternatives, is nurtured by traditions of Christian social thought. These call for care about all situations in which human dignity and justice are threatened. At present, the large, 'metaphysical' questions are all too frequently ignored,[43] rather than engaged by a critical analysis based on specific views of justice and human personhood.[44]

Understanding Surveillance Society

The chapters of this book are organized under three connected headings. In the first, *Situating Surveillance*, the growth of electronics surveillance is placed against the backdrop of modernity – its historical, social and cultural context. Given the huge scope of this task and that which follows it in the rest of the book, I draw upon illustrative material from a variety of sources rather than attempting to paint an exhaustive empirical picture. Two major issues are addressed in the remainder of the first part. First, do new technologies spell a qualitatively new surveillance? and secondly, if so does this add up to the emergence of a more authoritarian, prison-like society?

Part Two, *Surveillance Trends*, documents the specific ways in which surveillance is currently being augmented using new technologies, both in and between administrative and commercial contexts. Surveillance related to state functions takes up two chapters, as does surveillance in relation to capitalism, But wheras in other treatments the accent is on the productive sphere, in this book I lay great emphasis on the implications for surveillance of *consumption*. The role of computer matching, smart cards and universal personal identifiers is especially significant in this part of the book. Additionally, we shall see how surveillance has become very much a global, not just a national phenomenon, which also has implications for responses to it.[45]

In Part Three, *Counter-Surveillance*, the actual challenge of electronic surveillance is reappraised in the light of the analysis contained the first two parts of the book and the various responses to that challenge are examined and evaluated. Privacy is seen as one strand among others in an appropriate strategy of limiting electronic surveillance. Without for a moment minimising or dismissing the personal and social challenges of surveillance, however, I recommend the abandonment of merely negative, dystopian perspectives. They act as a hindrance to both adequate social analysis and appropriate ethical practice.

In order to understand the 'surveillance society', then, we must engage with several kinds of debate, and communicate across several different disciplinary areas. The sociologies of technology, politics and law are three such, but these in turn have to be seen in relation to debates over social control and surveillance on the one hand, and over modernity and post-modernity on the other. And none of these is satisfactorily discussed without reference to some concept of personhood, or some outline of what constitutes the good society.

Beyond mere 'understanding', however, sociology exists in close relation to its object of analysis , society. Sociology has become a crucial component of the social self-understanding, and thus also of the ongoing reproduction, of modern societies.[46] It is my hope that the analysis offered in these pages will make some small contribution to defining the social, political and cultural meanings of electronic surveillance so that, in dialogue with it, more room will be made for just, fair, loving and responsible social practice.