# Antisurveillance

BRIAN MARTIN

*Science and Technology Studies*
*University of Wollongong, NSW 2522, Australia*

ABSTRACT: Surveillance, a serious and growing issue, is essentially is a problem of unequal power. The usual reform solutions, such as codes of professional ethics, laws and regulations, give only an illusion of protection. Another approach, outlined in this paper, is to promote grassroots challenges to surveillance either through disruption or by replacing those social institutions that create a demand for surveillance. The institutional change programme provides help in choosing directions for present-day antisurveillance campaigns.

Is Big Brother watching you? George Orwell in *1984* warned against the dangers of an all-knowing, all-powerful government. The dangers of surveillance in societies today are not so stark. But the surveillance that actually goes on equals or surpasses many of Orwell's fears. Data is collected about citizens by dozens of corporations and government bureaucracies, including the police, taxation departments, marketing firms and banks.

Indeed, so central is surveillance that countries such as Sweden, Germany and the United States have been called 'surveillance societies'.[1] Yet few people are enthusiastic about the increased capacity of large organisations to collect information about themselves. Opinion surveys regularly show that most people attach great value to their own privacy – though not always to other people's privacy. It may be only a matter of time before latent concern about invasions of privacy crystallises into a mass movement against surveillance.[2]

So far, the main responses to the threat of surveillance – codes of professional ethics, laws and regulations – have given only an illusion of protection. These responses may be adequate in some circumstances, but they don't address the driving forces behind surveillance: power, profit and control. Codes of ethics seem to have made little impact, while laws and regulations are regularly flouted or made obsolete by technological change.

There is another approach, which has received relatively little attention: to challenge and replace the social structures that promote surveillance. My aim in this article is to outline a radical antisurveillance agenda. It is an exercise in thinking about massive changes in the organisation of society and especially in the distribution of power. Of course, this can be considered 'unrealistic' in the sense that such changes will be opposed by powerful groups and thus be difficult to achieve. But envisioning alternatives has the advantage of indicating directions for today's campaigns that will make some contribution to long-term

*Anarchist Studies* **1** (1993): 111-29

change. What is actually unrealistic is to imagine that the problem of surveillance can be addressed by band-aid methods.

In the following, I first give an overview of the problem and discuss surveillance as a problem of unequal power. Next, I describe the failure of reform solutions – that is, solutions implemented by powerful groups – and the limitations of technical fixes. Then I describe two grassroots programmes against surveillance, a 'disruption programme' and an 'institutional change programme'. The disruption programme is one designed to disrupt the process of surveillance, for example by corrupting databases. The institutional change programme is built around challenging and replacing social institutions that create a demand for surveillance. In conclusion, I argue that the institutional change programme provides help in choosing directions for present-day antisurveillance campaigns.

## THE PROBLEM[3]

Surveillance is not a new problem. The lack of privacy in small, intimate communities is notorious. What is new is invasions of privacy by large, remote organisations. There are two main factors here. First is the rise of large-scale bureaucratic organisations, both corporations and government bodies, in the past few hundred years. Second is the development of technologies for communicating at a distance and for collecting and processing large quantities of information. Computers and telecommunications are central here.

The capacities for collecting data about individuals are epitomised by the computerised database. There are thousands of such databases, including police files, military records, welfare files, marketing lists, taxation files, medical records and credit listings. Most of these are compiled when we fill out forms, such as a census form, an application for a loan, a registration for a hospital visit, enrolment at a school, an application for an automobile licence or a subscription to a magazine. Further information is added by banks (every deposit or withdrawal), doctors (each visit to a hospital), teachers (grades for all courses), and many others.

The capacity to manipulate databases on a computer allows invasions of privacy never imagined in earlier days. For example, many telephone directories are now available in computerised form. It is a simple matter to insert a telephone number and obtain the name and address. Marketeers can put in the name of a street and obtain a listing of the names and phone numbers of the people living there. These so-called 'reverse telephone directories' allow going from numbers or addresses to names, something not previously anticipated in compiling directories.

Police sitting in their patrol car can access computerised police files remotely. They can key in the licence number of a car that is being driven

dangerously, whose occupants 'look suspicious', or that is parked near a political meeting. They can receive information about the car owner's police record, and they can add information to the owner's file.

Databases are far from secure. Getting access to 'confidential' information is often a simple matter of connections or money. Private investigators routinely obtain information about credit ratings, police records, tax payments and the like by ringing up 'friends' in the relevant agency and making an appropriate payment.[4]

Lack of security is only one problem. Another is inaccuracy. Police repeatedly arrested one man for a crime he didn't commit; the real criminal had stolen his identification documents. In another case, a woman was repeatedly denied rental accommodation; it turned out that she was recorded on a credit-rating database as a bad risk due to defaulting from payments, although it was the owner who was to blame.

Individual databases are powerful tools. When they are linked to each other, enormous new potentials are created. For example, taxation records can be linked automatically to records of divorced parents who have failed to maintain court-specified child support payments. It is then a simple matter to extract the child support payments in the process of assessing income tax. The beauty of this approach, from the administrator's point of view, is that the defaulter cannot escape by leaving town, as surveillance operates on a national or even international scale.

More extreme cases have occurred. The computer records of a driver, stopped for speeding, can be checked and a demand made for payment of parking fines – or library fines. Lists of subscribers to magazines are commonly sold to other organisations; the subscribers then become targets for sales messages.

Newer telephone systems allow the telephone number of the caller to be registered by the receiver in a display. It is also possible to automatically record the caller's number. A company can offer a free gift to anyone calling a particular number and thus obtain a listing of all numbers that call up. The numbers then can be used for direct telephone solicitations. Telephone marketing can be partly automated, with a computer dialling the number and conducting at least the first part of the conversation.

With old-style printed files, a definite decision was required to search out information about someone in particular. It used to be that a bank teller would have to have some reason or suspicion before pulling out the file for a customer at the counter. Doing this for everyone would simply take too long. Computerised files allow routine checking. The system can be designed so that every time someone comes into a bank for a deposit or withdrawal, their file is retrieved in a matter of seconds – with, for example, the information that they are overdue on a loan repayment. What this means is that information on everyone is automatically checked: everyone is under suspicion.

Just as computers can store and manipulate information in ways impossible

previously, so other new technologies make it possible to collect ever more detailed and personal information about individuals. Bugging devices have been around a long time, but they are smaller, harder to detect and provide better quality transmissions than ever before. Video cameras are apparent in many shops, but there are also many that are not so apparent, for example hidden inside lights. For the serious snooper with enough money, the technological capabilities are awesome. Nightscopes can detect infrared radiation in order to see in the dark; sensitive sound receivers can listen in to conversations from outside a building, by deciphering the vibrations on a window pane in a room in which people are speaking; computer-to-computer communications can be intercepted and decoded; and many more amazing things.[5] Some of the opportunities for surveillance are open to virtually anyone. For example, it is easy to use radio receivers to listen in on a neighbour's conversations on a cordless telephone.

It is in the workplace that surveillance has long been greatest and where the new technologies are 'employed' to greatest effect. Word processors have their keystrokes monitored, and indeed computers are regularly set up to monitor any routine process. Open or hidden cameras are commonplace. Beyond this, employers are seeking deeper knowledge about their workers. Psychological tests are often used to select workers or, more commonly, to rule them out. Physical features are under scrutiny too, especially in the United States, where blood and urine tests are increasingly demanded as a condition of employment. Whether the aim is to screen out workers with communicable diseases (such as AIDS) or to detect users of illegal drugs, the effect is ever greater exposure of previously private information about individuals.

Gary Marx, author of some of the most insightful studies of surveillance, points out that new technologies overcome most of the natural barriers that protected privacy in the past.[6] Surveillance technologies can operate at a distance, penetrate darkness and go through physical barriers, as in the case of various listening devices. Surveillance is harder to detect than ever before, whether through hidden cameras or remote listening devices. Surveillance requires less labour than before, since technology now can do much of the work. For example, telephone taps used to require tedious listening of all conversations; now computers with voice recognition can be used to signal the presence of 'trigger' words such as 'bomb'.

Surveillance has long been a central feature of institutions of social control, notably prisons and mental institutions. New technologies allow this control to be extended into the community. In a number of countries, people can serve sentences at home, so-called 'home detention'. Typically, they wear electronic bracelets or anklets which communicate with a central computer, which monitors their nearness to the house. One of the arguments for such alternatives to prison is that they would reduce prison populations, but the reality is that an ever-larger number of people may be caught in the net of the criminal justice system.[7]

## SURVEILLANCE AND POWER

The above examples of surveillance today give an idea of the scope of the problem. How is the problem to be understood? There are various theoretical perspectives available. For my purposes, it is useful to analyse surveillance as a cause and consequence of inequality of power. The key issue is the surveillance of the less powerful by the more powerful.

The word 'surveillance' has connotations of nastiness, but a little reflection reveals that keeping a close watch on others is not inherently bad. For example, it makes sense to keep a close watch on small children to make sure that they do not get hurt. The same applies to the sick and infirm. Many people appreciate someone watching out for them when they are doing something that is potentially risky, such as swimming in the sea or climbing a tall ladder. These are examples of 'surveillance' which can be most welcomed.

When people live together, they observe a lot about each other, and this can be considered a type of surveillance. It occurs in families, among friends, and in close-knit communities. Some of the attention in these circumstances may be resented, but much of it is an inevitable consequence of living as a member of a community. It can be a joy to see friends along the street or in a restaurant or to have them visit your home, even though they thereby know more about what you are doing at any particular time.

Most people are not concerned about 'surveillance' in such situations. Why not? In some of the cases, such as meeting friends, there is both a mutual agreement to participate and a rough equality of power. But in the case of a parent and a small child, there is an enormous difference in power and no real possibility of informed consent on the child's part. What makes the close watching in this situation acceptable is the trust implicit in the relationship: the trust that the parent will look after the child. (Of course, this trust may be violated, as when a parent beats or sexually abuses a child. Such actions provide justification for others, whether family, friends or the state, to intervene.)

What is normally called surveillance then applies to cases when either there is a substantial power difference or a lack of a trust relationship, or both. A large powerful organisation that collects data on individuals is a typical case. The organisation is able to collect data because it is powerful and becomes more powerful because of the data.

Is the fundamental problem the surveillance or the inequality in power? They are linked, so perhaps these two things can't be easily distinguished.

Note that I have couched this discussion in terms of surveillance and power rather than in terms of privacy and individual rights. Many of the writers in this area focus on privacy, assuming that there is a right to privacy and that violations of individual privacy must be weighed up against other competing values (such as increasing efficiency or stopping crime). This language of privacy and rights is typical of liberalism. It assumes that individuals are isolated entities who have

agreed to participate in society according to a 'contract'.

There are a lot of problems with this picture. Individuals are not isolated and autonomous but are inevitably products of and participants in society. Futhermore, few individuals can be said to have genuinely agreed to their place in society – as if there were any real alternative!

Another problem with the focus on privacy is that privacy means different things to different people and means different things in different cultures. (Even so, there may be commonalities in attitudes to privacy across the most divergent cultures.[8]) But people who have different concepts of privacy may agree to oppose particular types of surveillance.

A focus on privacy directs attention to the individual whose privacy is invaded; a focus on surveillance directs attention to the exercise of power and to the groups that undertake it. For these reasons, antisurveillance is a better rallying point than privacy.

## REFORM SOLUTIONS

One way proposed to protect privacy is to ensure that all the people who have access to information collected about members of the public deal with it in a 'responsible' fashion. This means that those who deal with or have responsibility for information – such as computer administrators, police, government bureaucrats, telephone technicians and personnel managers – should have the highest personal standards. For example, they should use the information only for the purposes for which it was collected. Ethics codes are sometimes proposed to set a standard of behaviour.

Critics are entitled to be sceptical about claims that there is no problem because there is a stringent code of professional practice or because all those with access to confidential information have the highest ethical standards. To be fair, most bank managers, marketeers, hospital administrators and the like are responsible people who would be most unlikely to misuse the information at their disposal. But all it takes is a minority of less responsible people for serious breaches of confidentiality to occur.

However, even if every single person with access to confidential data were absolutely trustworthy, this would not solve the problem. This is because there are enormous bureaucratic pressures to extend the use of data about individuals for, from the organisation's point of view, very sound reasons. The tax office wants to collect data to ensure that all pay their fair share of tax, so that enough money is available for essential public spending. Government bureaucracies keep data on welfare recipients in order to make sure that only those who really need benefits actually receive them; with limited funds, making payments to those who don't need them means less for those who do. Marketeers collect information on consumers in order to increase their profits, to be sure, but they

sincerely believe they are aiming to provide a better service or product to those who really need it. Police see surveillance as necessary to protect the community from serious crime.

One may argue that these attitudes are rationalisations for policies that benefit those defending the surveillance, namely the salaries of government bureaucrats, etc. But it would be unfair to accuse people of bad intentions. It is only a tiny minority of snoopers who gather information for the purpose of blackmail. Almost all surveillance is carried out by well-meaning people with what they believe are the most worthy ends in mind.

Furthermore, there is a lot of public support for surveillance to stop cheats and crooks. Bureaucratic and popular pressures often reinforce each other, egged on by media stories of welfare abuse or dangerous criminals.

When a government department proposes to compare tax records with lists of recipients of unemployment benefits, a central motivation is to save money by exposing those on good salaries who are also improperly obtaining unemployment payments. What could be more sensible, indeed laudable? Ensuring that everyone in the system is highly responsible will cut out some of the clear-cut abuses but will not address the bureaucratic and commercial pressures for ever greater collection and combination of data about individuals.

Another way of opposing surveillance is for governments to pass laws and establish agencies and systems to protect privacy. Indeed, this seems to be the favoured approach by many writers on privacy. Laws, regulations and privacy commissions can, indeed, accomplish many things. They can allow citizens to see and correct files held on them; they can outlaw certain practices, such as sharing of databases; they can ensure that privacy considerations become a factor in policy making; they can establish organisations that keep tabs on technical developments; they can impose penalties on violators of people's privacy.

This sounds well and good. The people who propose and implement these solutions are undoubtedly well-intentioned. But the whole approach is fundamentally flawed.

One big problem is that the path of legal regulation assumes a trade-off between privacy and other benefits, such as profit or bureaucratic efficiency. In the balance, privacy usually comes off second best. There are clear and direct advantages to corporations and government departments in expanding their capacities to gather and manipulate information on citizens. By contrast, there are few powerful groups with any direct interest in protecting the privacy of the 'ordinary citizen.' The result is that privacy concerns are routinely squashed by the steamroller of surveillance.

It is risky to rely mainly on governments to provide protection against surveillance when governments themselves are responsible for much of it. The very existence of the government depends on collecting taxes. So when government needs for tax money meet citizen resistance to further impositions, it becomes difficult to argue against extra measures to stop 'tax cheats', even when

these measures involve accumulating ever more information about individuals. The state also depends for its existence on the police, military and spy agencies to detect and thwart external and internal challenges. These arms of the state are well known to thrive on information collected through surveillance.

In practice, the main role of laws protecting privacy may be to give the illusion that the problem is being dealt with. Certainly that is the case for the Privacy Commission in Australia, whose task is to make recommendations on how to maintain privacy within the present laws. The Commission can do nothing to challenge existing laws. So when the Australian government decided to allow tax records and other records to be combined – something it had earlier promised not to do – the Privacy Commission could only sit there and make recommendations within the framework of the new policy.

It is unrealistic to expect governments to take the lead in countering the driving forces behind increasing surveillance. True, the state is not a unified entity, so there can be groups inside pushing against as well as for surveillance. But as long as the state depends fundamentally on maintaining power over citizens – and it must, in order to extract resources to support itself and to defend itself against internal and external enemies – the state cannot be a reliable ally against surveillance, since the power of the state is a prime beneficiary of surveillance activities.

## TECHNICAL SOLUTIONS

Another way to deal with problems of surveillance is to implement technical fixes. An example is public key encryption for electronic communications.[9]

Consider a person who uses a computer to generate a message that is communicated through the telephone network to another computer. Surveillance of this message is possible by tapping into the network and deciphering the computer text. Now add encryption: the sender uses a little programme to turn their message into code, using their own private key and the receiver's public key. The receiver is able to decipher to message by using the receiver's private key and the sender's public key. The receiver also knows that the message could only have come from the sender, for whom the key thus is an electronic signature. This method requires a fair bit of computing power but could be cheap if mass produced.

Naturally, spy agencies do not like it. The United States National Security Agency has pushed for keys designed by the NSA itself. Others suspect that the NSA will design the key so that it can break the code and be able to read all telecommunications. Individual users, by contrast, want a system to guarantee the integrity of their messages.

Many government and corporate elites won't be attracted to public key encryption either. They prefer encryption systems which ensure that they can

find out what their employees or clients are communicating.

The first lesson from this debate is that technical solutions are not automatically implemented, however logical they may appear. Technical approaches to collecting and processing information are the product of the exercise of power. In the case of public key encryption, the power struggle is visible. Usually such struggles are not.

Technical choices pervade privacy issues. They are involved in designing questionnaires and standard forms (why should I have to provide my social security number when assigning copyright of an article to a publisher?). They are involved in setting up computer databases. They are involved in establishing standards for telecommunications systems. These and other technical choices involve the exercise of power. A technical fix is not an easy solution to the problem of surveillance, but simply another arena for the same basic debates.

## DISRUPTING SURVEILLANCE

Surprising as it may seem, much surveillance depends on cooperation or acquiescence by the person about whom information is collected, such as when we fill out forms. As well, the cooperation or acquiescence of various workers is required for surveillance to be successful. These dependencies suggest a number of measures to corrupt databases. (I will comment afterwards on the disadvantages of this approach.)

- Disrupters can fill out forms with small mistakes in their names, addresses, and other details. This will create multiple entries in databases and make it more difficult for database matches to be successful.
- Disrupters can fill out forms with imaginary information, or with information about famous people (or about database managers). This will swamp the database with incorrect information.
- Workers who key in data from forms can introduce mistakes.
- Computer programmers can corrupt files. A subtle approach is to make changes that reduce the value of files, for example replacing the occasional number '0' by '1' or replacing the occasional letter 'a' by 'e'. (Just imagine how this would affect a record of personal data about yourself.)
- Computer programmers can take more drastic action against files, for example totally erasing databases (and backup copies). There are a number of techniques, such as logic bombs, Trojan horses and computer viruses, all of which can be most destructive.
- One needn't be a computer specialist to be disruptive. A magnet can be quite sufficient to damage computer tapes and discs, and pulling out a few circuit

boards can disable a computer.

- In the face of direct surveillance by bugs or observation, a range of devious techniques can be imagined, such as disguises and misleading taped messages.

These sorts of antisurveillance tactics are in the great tradition of the Luddites, who are remembered for smashing the machines that put them out of work but who had a much more developed political programme than is usually recognised. In assessing the disruption programme for antisurveillance, it is worthwhile to mention some contemporary sabotage activities. A considerable amount of workplace sabotage occurs, almost entirely on an individual basis.[10] There is little in the way of an organised movement to use such disruptive tactics. There is, though, some advocacy. The magazine *Processed World* has given sympathetic treatment to office workers who subvert business-as-usual through workplace sabotage.[11] David Noble has written the most sophisticated argument for such techniques as a way for workers to challenge the power of management and capitalism.[12]

Methods of sabotage have been adopted openly by radical environmentalists under the banner of Earth First!, with the goal of protecting wilderness from governments and corporations. The practical manual *Ecodefense*[13] describes techniques for pulling out survey stakes, defacing billboards, spiking trees and incapacitating bulldozers, among others. They advocate only those techniques which avoid any risk of injury to others. Their first priority is not to be caught. It should be noted that Earth First!ers also use a range of open and nondestructive methods, such as rallies and sitting in trees.

Corrupting databases and other ways of disrupting surveillance provide a challenge to the encroachments of the surveillance society, but they have a number of limitations. Introducing errors into databases sounds effective, but databases are full of errors already. How much difference would more errors make? The impact would need to be financially significant (even more wrong names on mailing lists!) or politically potent (names of powerful people on embarrassing lists).

More importantly, disrupting surveillance in this fashion is, by necessity, mostly a private activity. It provides a poor basis for mobilising a social movement; instead, it tends to breed secrecy and vanguards. Furthermore, such secret activities are ideal for the duels of spy versus counterspy. When it comes to spying and infiltration, social movements are likely to come off second best to state agencies.

This was certainly the case with Earth First!, which was infiltrated by the FBI. Some Earth First!ers have renounced sabotage and secret tactics and, as a result, been able to forge links with workers in a way impossible using individualist, secretive methods.

Instead of disrupting surveillance carried out *by* powerful organisations,

another approach is to mount 'countersurveillance': surveillance *of* powerful organisations. Today, large organisations and powerful individuals have as much privacy as money will buy, and most surveillance is carried out against the weak, disorganised and defenceless. The builders of weapons of mass destruction use every available means to ensure secrecy while spying on their enemies (foreign powers and peace movements). Can this pattern be challenged and reversed by promoting surveillance of the rich, powerful and dangerous?

The challenge is enormous, but some courageous individuals and groups have made efforts in this direction. A few investigative journalists have probed the corridors of power. Their exposés are incredibly threatening to organisational elites simply because they reveal what is actually happening on the inside. Such information undoubtedly contributes to better strategies by social movements. Many more exposés are needed. Even more daring is spying on spies and publicising the results, such as the efforts of the magazine *Counterspy* to expose CIA agents. This was so threatening to the spy agency that special legislation was passed to stop such revelations.

Much more could be said of the potential for disrupting surveillance. The techniques to do this deserve much more study and experimentation. It does seem, though, that they offer at most one part of a solution: they interfere with surveillance but do not offer an alternative to the systems that generate and thrive on it. Furthermore, as the experience of Earth First! has shown, disruption sometimes triggers increased surveillance and repression. If it is important to make the means to achieve a society with less secrecy compatible with the goal, then disruption is far from an ideal approach.

## INSTITUTIONAL CHANGE

Here I outline some radical approaches to eliminating surveillance by eliminating the institutional capacity or need for it in the first place. By necessity, this is an extremely brief overview, but it should be sufficient to indicate the general approach.

Many of the proposals here, such as 'abolish nuclear weapons' or 'abolish the state', are easy to say but very difficult to accomplish. After all, it's a challenging, long-term process to succeed in abolishing nuclear weapons, not to mention abolishing the state. It is not my intention to present strategies for achieving these goals; in most cases, there are well-established perspectives or movements for doing so. Rather, my intention is to point out the institutional sources of surveillance in order to inform campaigns against surveillance, so that they can be chosen and implemented in ways which weaken rather than strengthen the institutional roots of surveillance.

To put this another way: abolishing nuclear weapons or the state is not a prerequisite for eliminating surveillance. Rather, campaigns against nuclear

weapons or the state should be developed so that they are compatible with struggles against surveillance, and campaigns against surveillance should be developed so that they are compatible with struggles with the ultimate aim of abolishing nuclear weapons, abolishing the state or eliminating other roots of surveillance. In short, the institutional change programme provides a *direction* for antisurveillance campaigns today. These and other implications will be elaborated in the final section.

**Dangerous technologies.** Surveillance has been justified by the need to protect against the dangers of technologies. Given the existence of the technologies, surveillance makes a lot of sense. One way to eliminate the surveillance is to eliminate the technologies.

Military spying is needed to protect against unauthorised access to nuclear and other weapons. The solution is to abolish these weapons.

Nuclear power is potentially dangerous. Hazards include reactor accidents, terrorist use of nuclear materials and proliferation of nuclear weapons capabilities through 'civilian' nuclear programmes. Nuclear power therefore brings with it the necessity for surveillance. There have been special police forces for nuclear facilities, as well as spying on anti-nuclear power groups. One of the earliest objections to nuclear power was the tendencies towards a police state inherent in a nuclear society.[14] The solution is straightforward: abolish nuclear power.[15]

A more commonplace dangerous technology is the car. The danger of traffic accidents has engendered a multitude of traffic regulations and the attentions of police. There are laws requiring wearing of seat belts and laws prohibiting high blood alcohol levels. The automobilised society thus brings with it considerable invasions of personal privacy. Cameras already watch over dangerous intersections. As well, there are proposals to introduce automatic electronic identification of road vehicles, in order to reduce congestion or charge for road use, or both. A computer would record when your car passes a monitor underneath or beside the road.

Far from cars enjoying 'freedom of the road', they actually do more than any other technology today to put people on police files. The solution is to move towards a society in which cars play a much smaller role. Proper town planning, which makes it easy for people to live affordably near workplace, shops and amenities, can greatly reduce the need for cars, and make walking and cycling much more attractive. For longer distances, cheap public transport offers a service without the rationale that surveillance is needed to avoid accidents.

**Medical records.** Records of a patient's medical treatment can, in the wrong hands, be used to embarrass or discriminate against them. The simple solution is for patients to keep their own medical files. They could, if desired, give copies to anyone they trusted, whether a family member, a friend, their doctor or indeed a hospital.

**Prisons.** Prisons are the ultimate in surveillance. The prisoner is both constrained and observed. There are several ways to reduce the number of

prisoners and hence the extent of surveillance. One is to abolish victimless crimes, such as for vagrancy and drug use. Another is to increase social equity, so that there is less incentive for crime. The ultimate aim should be to abolish prisons. After all, they do not reduce the crime rate and are an insult to human dignity. Prisons should be replaced by a range of methods and policies genuinely oriented towards rehabilitation.[16]

**Workplaces.** Workers are monitored on the job by management to maintain output but also to keep workers under control. The alternative is for workers to control their own work collectively. This includes semi-autonomous work groups which decide the way they will do a job within the general framework decided by management. It includes collectives, in which all workers as a group make the crucial decisions about what to produce and how to carry out their jobs. It includes workers' control – usually associated with larger organisations – in which workers make the basic decisions about their enterprise and work, using decision-making methods including voting, delegate systems, and rotation through managerial positions.[17]

It should be noted that under workers' self-management, what a worker does is still watched by others. The difference is that it is workmates who do the watching, not managers. This is a change in the distribution of power. Self-management should be distinguished from techniques such as Total Quality Management, which also involve workers watching each other, but in a system designed by management to extract the greatest profit while maintaining managerial control.

**Spy agencies.** Organisations such as the FBI, MI5 and KGB, which are found in countries throughout the world, are responsible for some of the most objectionable snooping. They escape serious scrutiny by claiming the higher needs of 'national security'.

There is a simple solution to surveillance by spy agencies: the agencies should be abolished. These organisations mainly serve their own ends and the ends of national elites. The chief targets of spy agencies are not foreign spies but domestic citizens. There has never been an open and honest assessment of their value to the wider community: such assessments are prevented by secrecy provisions.

What about preventing terrorism? Spy agencies have probably done more to promote than to prevent terrorism – especially remembering that most terrorism is carried out by governments. A grassroots antiterrorism programme would include serious attention to the grievances of minority groups (whose members may resort to terrorism to gain a hearing) and community-level communications and solidarity.

What about defence secrets? These should be made obsolete by abolishing the military and replacing it with community-based methods of nonviolent defence, which require little or no secrecy.[18]

**Government services.** Data is collected by governments to make sure that

recipients of services are genuine. This applies to unemployment benefits, child support schemes, pensions for disabled people, war veteran benefits, education support schemes, health benefits, and the like. Keeping detailed data on recipients is considered essential to prevent cheating, in order to keep costs down.

One solution is to provide basic services free to anyone who wants them. This applies today to services such as public parks and public libraries. Why not also to food, shelter, health services, etc.? The basic principle is that services for identified individuals are replaced by collective provision, for which there is no need for individuals to be identified.

To address the ramifications of such changes would be an enormous task. Let me outline a few cases. Consider food. Basic staples could be provided at community centres to anyone who wanted them (possibly with donations invited to help cover costs). This would be quite possible with today's production, which is more than ample to feed everyone if distributed appropriately (including in most of the poor countries where people die of starvation).[19] In many countries, governments control markets in order to limit production. Such schemes would become unnecessary.

Consider health services. The escalation of costs here comes primarily from intensive interventions using expensive technology. Most of the services that make a big difference to people's health don't have to cost a lot. Generic drugs could be provided free or at nominal cost. Many more people could be trained to administer basic health care. Emphasis could be shifted from curative methods to prevention by improving diet, exercise and occupational health and safety.

**Private investigative agencies.** Private agencies undertake a significant amount of surveillance, but it is small in volume compared to listening operations and databases by governments and large corporations. But the private agencies usually are collecting information about a particular individual, and so their actions tend to be particularly objectionable.

A large fraction of private spying is for the purpose of bolstering a disputed claim. For example, an insurance company may hire a company to watch a person who has claimed to have received a back injury at work. Films of the person playing golf or putting out the wash can then be produced in court to undermine the compensation claim.

The incentive for this sort of spying comes from fault-based compensation systems: if the employer is responsible, then there's a big payout to the worker. Fault-based systems are common in areas such as military veterans' benefits, divorce proceedings and automobile accidents as well as workers' health. The solution here is to eliminate fault-based compensation systems. No-fault systems work quite well in many countries.

**Commercial databases.** Companies collect an enormous amount of information on potential consumers, which they use to help design products and marketing strategies. Banks and credit agencies collect information on credit worthiness. A future cashless society with widespread use of electronic funds

transfer for purchases would leave an electronic record of consumer behaviour unprecedented in detail.

Large corporations in a market will inevitably become involved in mass marketing. The availability of cheap and powerful computing capabilities means that the extensive use of databases is impossible to control in this situation. There are two institutional revolutions that would undercut the drive for consumer surveillance: abolishing large corporations and abolishing the market, or both.

Abolishing large corporations but retaining markets is a vision of many libertarians and free-market anarchists. (Also essential for their project is reduction of the state to a minimal set of functions.) In an economy in which large bureaucratic organisations are not viable, entrepreneurs would mainly trade in local or specialist markets. An individual entrepreneur would undoubtedly collect information about potential buyers and sellers. But the potential dangers of large databases would be minimised, because the various buyers and sellers in the market would have similar, limited degrees of power. The unequal relationship of the large, powerful corporation vis-a-vis the individual consumer would be eliminated.

An alternative way to undermine commercial surveillance of consumers is to abolish the market and replace it by local self-management by workers and community members. (In this vision, the state is totally eliminated.) This is the project of anarchists or, in other words, libertarian socialists. In this model, the production and distribution of goods and services is done on a cooperative basis, rather than the competitive principles built into the market. Various cooperative enterprises would undertake tasks of necessity to the community, deciding for themselves, in consultation with other enterprises and organisations, priorities and methods.[20]

In such a system, there would be no incentive to collect information about large numbers of isolated consumers, since marketing in the capitalist sense would not exist. More importantly, power relationships would be much more equal, so that the foundation for surveillance would not be present.

**Taxation.** Governments are built on taxation. Without taxation – or, more generally, the extraction of resources from the economy – the state could not exist. In earlier eras, governments could survive without taxing most individuals, using only excise duties and taxation of large estates. But as the modern state expanded in size and power with the triumph of capitalism over feudalism, the demand for more and more information about individual citizens also expanded. This is not just to collect taxes but also to distribute government services, which provide the justification for the state.

Computers have added extra technological capabilities to the state's thirst for information, but the thirst was there long before computers. The rise of the modern state was a process of central bureaucracies entering communities, collecting information, assessing taxes and conscripting soldiers.[21]

Since surveillance is central to the existence of the state, reform is hardly

enough. The radical solution is to abolish the state. The alternative is communities organised around self-management, as outlined above.[22]

## FROM VISION TO STRATEGY

This institutional change programme is radical, going to the roots of the problem of surveillance. It is hardly a practical proposition, though, to implement these solutions through a short, sharp campaign. What use, then, is the programme?

First, it draws attention to the way that surveillance is deeply embedded in today's social institutions and is becoming more and more pervasive. The real idealism is to imagine that the problem can be solved by legislative and regulatory measures by the very institutions that are responsible for the problem. The radical agenda should warn against investing too much energy or hope in reform efforts, which may give only an illusion of protection.

Second, the programme provides an additional argument to challenge and replace hierarchical social structures. Alone, the problem of surveillance is hardly serious enough to question the value of nuclear power, corporate capitalism or the state. But surveillance is an important factor which should not be neglected in a focus on environmental impacts, war or exploitation of workers.

Third, the programme highlights the range of triggers for surveillance: 'national security,' marketing, protection against dangerous technologies, provision of welfare. There is no evil agency that is responsible for all surveillance; in this respect Orwell's *1984* is much more totalitarian than today's society.

Undoubtedly, most surveillance is carried out with the very best of intentions: to protect the nation, to provide better products to consumers, to economise on government expenditure. Surveillance is not a product of evil schemers. The debate over surveillance concerns different conceptions of the good.

Fourth, the programme of radical solutions provides a *direction* for campaigns today. While it is impossible to introduce collective provision or to abolish the state overnight, it is quite sensible to examine campaigns to see whether they aid the capacity for community self-reliance and whether they weaken rather than strengthen the power of the state.

**A sample campaign.** One way to mesh the disruption programme and the institutional change programme is to campaign for 'transparent organisations.' Consider a hypothetical egalitarian society whose policies ensure that privacy is maintained except when there is a potential for concentrations of power. In such a society, the activities of ordinary individuals and small groups would be considered private matters, but activities of any sizeable organisation would be totally open for inspection. Similarly, the activities of most people in most circumstances would be considered private matters, but the activities of individuals in positions of power or responsibility would be open for scrutiny. For

example, a person acting as a delegate representing a large number of people could not expect the same degree of privacy in their delegate role as in other circumstances.

The hypothetical egalitarian society, having renounced weapons of mass destruction as inhuman and incompatible with equality, might institute procedures for monitoring certain types of technological development, to prevent creation of new destructive weapons. In other words, there might be surveillance against new methods of oppression. It is easy to see that in such a society, the relation between information and power would be the reverse of what it is in today's society.

The demand that large organisations be completely open to scrutiny is, in effect, a demand that organisational elites relinquish much of their power over both subordinates and outsiders. This demand thus is a challenge to both surveillance systems and their institutional roots.

The primary aim in a campaign for transparent organisations is to undermine the legitimacy of organisational secrecy ('privacy' is the wrong word) while maintaining the legitimacy of individual privacy. With less legitimacy, disruption of surveillance systems would come to be considered acceptable, even admirable. Institutional change would become more viable. Workers could organise more effectively. Spy agencies would be under threat. If organisational elites were exposed to intense scrutiny, they would be much more likely to favour systems that provided services without discrimination, such as collective provision.

A campaign for transparent organisations is not without difficulties. For example, how is one to distinguish between a worker's private and organisational activities? Whether campaigning for transparent organisations is a useful approach, or whether some other approach will work better, can only be determined by the test of practice. Be assured, the test of practice will be a tough one. Nothing is more certain than that opponents of surveillance will come under the most intense scrutiny of all.

## NOTES

I thank Stan Aungles, Richard Badham, Sharon Beder, Jim Falk, Oscar Gandy, Jr., Richard Joseph, Dave Keenan, Gary Marx, Jim Rule, Pam Scott and an anonymous referee for helpful comments and discussion.

[1] Flaherty 1989.

[2] Gandy 1989.

[3] See, among others, Bennett 1991; Burnham 1983; Campbell and Connor 1986; Clarke 1988; Flaherty 1989; Gandy 1989; Laudon 1986; Linowes 1989; Marx 1988; Rule et al. 1980; Rule et al. 1983; Wicklein 1981.

[4] See, for example, Independent Commission Against Corruption 1992.

[5] On the other hand, not all fancy new technologies are as effective as promotional material may assert or fearful targets may believe.
[6] Marx 1986.
[7] Cohen 1985.
[8] Moore 1984.
[9] Finney 1993.
[10] Sprouse 1992.
[11] *Processed World*, 41 Sutter St. #1829, San Francisco CA 94014, USA.
[12] Noble 1983.
[13] Foreman and Haywood 1988.
[14] Jungt 1979.
[15] Eliminating nuclear weapons and nuclear power would still leave the problem of nuclear waste, for which 'surveillance' would be required. But surveillance of waste is a different matter from surveillance of individuals, not raising quite the same issues of power inequality.
[16] Mathiesen 1990.
[17] Hunnius et al. 1973; Mattick 1978; Roberts 1973.
[18] Boserup and Mack 1974; Martin 1993; Sharp 1990.
[19] George 1977; Lappé et al. 1977.
[20] See, for example, Thornley 1981.
[21] Jacoby 1973; Tilly 1975.
[22] See, for example, Bakunin 1971; Guérin 1970; Ward 1982.

## REFERENCES

Bakunin, Michael 1971. *Bakunin on Anarchy* (edited by Sam Dolgoff). New York: Vintage.

Bennett, Colin J. 1991. Computer, personal data, and theories of technology: comparative approaches to privacy protection in the 1990s. *Science, Technology, and Human Values* **16**(1): 51-69.

Boserup, Anders and Mack, Andrew 1974. *War Without Weapons: Non-violence in National Defence*. London: Frances Pinter.

Burnham, David 1983. *The Rise of the Computer State*. London: Weidenfeld and Nicolson.

Campbell, Duncan and Connor, Steve 1986. *On the Record: Surveillance, Computers and Privacy: The Inside Story*. London: Michael Joseph.

Clarke, Roger A. 1988. Information technology and dataveillance. *Communications of the ACM* **31**(5): 498-512.

Cohen, Stanley 1985. *Visions of Social Control: Crime, Punishment and Classification*. Cambridge: Polity Press.

Finney, Hal 1993. Protecting privacy with electronic cash. *Extropy*, No. 10, Winter/ Spring: 8-14.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill: University of North Carolina Press.

Foreman, Dave and Haywood Bill (eds.), 1988. *Ecodefense: A Field Guide to*

*Monkeywrenching*. Tucson, AZ: Ned Ludd Books, second edition.
Gandy, Oscar H. Jr. 1989. The surveillance society: information technology and bureaucratic social control. *Journal of Communication* **39**(3): 61-76.
George, Susan 1977. *How the Other Half Dies: The Real Reasons for World Hunger*. Montclair, NJ: Allanheld, Osmun.
Guérin, Daniel 1970. *Anarchy: From Theory to Practice*. New York: Monthly Review Press.
Hunnius, Gerry; Garson, G. David and Case, John (eds) 1973. *Workers' Control: A Reader on Labor and Social Change*. New York: Vintage.
Independent Commission Against Corruption, 1992. *Report on Unauthorised Release of Government Information* . Sydney: The Commission.
Jacoby, Henry 1973. *The Bureaucratization of the World*. Berkeley: University of California Press.
Jungt, Robert 1979. *The New Tyranny*. New York: Grosset & Dunlap.
Lappé, Frances Moore and Collins, Joseph with Cary Fowler 1977. *Food First: Beyond the Myth of Scarcity*. Boston: Houghton Mifflin.
Laudon, Kenneth C. 1986. *Dossier Society: Values Choices in the Design of National Information Systems*. New York: Columbia University Press.
Linowes, David F. 1989. *Privacy in America: Is Your Private Life in the Public Eye?* Urbana: University of Illinois Press.
Martin, Brian 1993. *Social Defence, Social Change*. London: Freedom Press.
Marx, Gary T. 1986. The iron fist and the velvet glove: totalitarian potentials within democratic structures. In James F. Short, Jr. (ed.), *The Social Fabric: Dimensions and Issues*, pp. 135-162. Beverly Hills: Sage.
Marx, Gary T. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.
Mathiesen, Thomas 1990. *Prison on Trial: A Critical Assessment*. London: Sage.
Mattick, Paul 1978. *Anti-Bolshevik Communism*. London: Merlin.
Moore, Barrington Jr. 1984. *Privacy: Studies in Social and Cultural History*. Armonk, NY: M. E. Sharpe.
Noble, David 1983. Present tense technology. *Democracy* **3**(2): 8-24; 3(3): 70-82; 3(4): 71-93.
Roberts, Ernie 1973. *Workers' Control*. London: Allen and Unwin.
Rule, James; McAdam, Douglas; Stearns, Linda and Uglow, David 1980. *The Politics of Privacy*. New York: Elsevier.
Rule, James; McAdam, Douglas; Stearns, Linda and Uglow, David 1983. Documentary identification and mass surveillance in the United States. *Social Problems* **31**(2): 222-34.
Sharp, Gene with the assistance of Bruce Jenkins 1990. *Civilian-Based Defense: A Post-Military Weapons System*. Princeton: Princeton University Press.
Sprouse, Martin with Ely, Lydia (eds) 1992. *Sabotage in the American Workplace*. San Francisco: Pressure Drop Press.
Thornley, Jenny 1981. *Workers' Co-operatives: Jobs and Dreams*. London: Heinemann.
Tilly, Charles, (ed.) 1975. *The Formation of National States in Western Europe*. Princeton: Princeton University Press.
Ward, Colin 1982. *Anarchy in Action*. London: Freedom Press.
Wicklein, John 1981. *Electronic Nightmare: The Home Communications Set and Your Freedom*. Boston: Beacon Press.