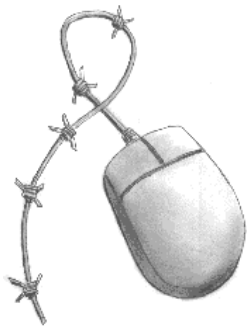
Participating With Safety Briefing no. 7

Living Under Surveillance



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

This is one of a series of briefings on Participating Safely Online. This briefing covers:

- Surveillance and counter-surveillance
- Official and un-official telephone tapping
- Monitoring mobile phones and post
- Bugs and computer-based surveillance
- Photography, documentation trails
- Tips for basic counter-surveillance

Surveillance and counter-surveillance

Surveillance is the art of monitoring the activities of persons or groups without them knowing they are being monitored. Surveillance has been an intrinsic part of human history. Sun Tzu's *The Art of War*, written 2,500 years ago, discusses how spies should be used against a person's enemies. But modern electronic and computer technology have given surveillance a whole new means of operation. No longer must it be practised by agents, it can be automated using computers. No longer do people have to be watched - their own activities create records that describe their activities.

Counter surveillance is the practise of avoiding or making surveillance difficult. Before computer networks, counter surveillance involved avoiding agents and communicating secretly. With recent development of the Internet and computer databases counter surveillance has grown. Now counter surveillance involves everything from knowing how to delete a file on a computer to avoiding becoming the target of direct advertising agencies.

The greatest impact of computer-enabled surveillance is the numbers of organisations involved in surveillance operations:

- The state and security services still have the most powerful surveillance systems, because they are enabled under the law. But today levels of state surveillance have increased, and using computers they are now able to draw together many different information sources to produce profiles of persons or groups in society.
- Many large corporations now use various form of 'passive' surveillance. This is primarily a means of monitoring the activities of staff and for controlling public relations. But some large corporations actively use various forms of surveillance to monitor the activities of activists and campaign groups who may impact their operations.

- Many companies trade in information lawfully, buying and selling it from other companies or local government agencies who collect it. This data is usually bought by companies who wish to use it for marketing or advertising purposes.
- Personal information is obtained my many small groups and individuals. Some of this is for harmless purposes, but increasingly sensitive personal information is being obtained for criminal purposes, such as credit card and other types of fraud.

For those who are peacefully working to change society, surveillance presents a problem. Particularly after the September 11th attack on New York, many states now view political dissent as a problem, and have introduced new laws to strengthen their surveillance powers. Many states have also redefined their legal definition of terrorism to not only include violent acts, but also types of direct action protest. Even where groups have no involvement in violence, states and corporations may try to use information obtained about groups or individuals to discredit their work. As the scope of surveillance increases, it is important that groups and individuals manage their exposure to different types of surveillance to limit the damage it can do to them, or their work.

Modern surveillance cannot be totally avoided. If the state use all of their resources to investigate your activities, they will be able to do so. However, non-state groups may employ surveillance techniques against your organisation, and some precautions can reduce their success.

This briefing explores the means by which the impacts of surveillance may be lessened. This briefing is meant to be used as the basis of discussion, and not as a complete counter-surveillance manual.

Note: In all the forms of surveillance mentioned below, the issue of *patterns* is important. Although in isolation a single piece of communications data seems useless, when collected together with the communications data of other people it can disclose a lot of information about organisational relationships, work patterns, contacts and personal habits. The collection and processing of communications data is largely automated using computers - hence easy to do.

Telephones

The official tapping of telephone lines

The contracts or licenses by which the state controls telephone companies means that they must provide access for tapping lines to the security services and the police.

When telephone exchanges were mechanical a tap had to be installed by technicians, linking circuits together to route the audio signal from the call. Now that many exchanges are being converted to digital technology installing taps is far simpler, and can be done by installing small plugs, or even by computer. Telephone services provided by cable TV companies are tapped in a similar way.

Unless the tap has been very badly installed, it is not possible to tell if your line is being tapped or not. The noises that some people believe to be telephone taps are really just noise created by the induction of signals from other phone lines. Because the tap is made at the exchange it is very difficult to tell if the line is tapped because there will be no appreciable difference in volume. But irrespective of the tapping of content, communications data will always be collected automatically, and stored for later use by the billing department of your phone company or the security services.

For telephone services run via digital exchanges, the information generated will consist of a list of the phone numbers you have called, the duration of the calls, and perhaps a log of the type of communications media being used (some services send data and voice communications via different routes to conserve

bandwidth).

The unofficial tapping of telephone lines

It's also possible to be tap conversations unofficially. There are a number of ways to monitor telephone conversations:

- Recording the conversation - the person making/receiving the call records the conversation using a 'telephone pickup coil' attached to the ear-piece, or they fit an in-line tap with a recording output. Both of these are easily available through electrical shops. Most who record telephone conversations, such as journalists, will use the recording for their own private work. But be aware that anything you say to someone you don't know may be recorded and used for other purposes.
- Direct line tap - this is what the state do via the telephone exchange. But unofficial tapping, where the user's line is physically tapped near the house, is also possible. The tap can either involve a direct electrical connection to the line, or a coil placed around the line to pick up the signal inductively. There will be some drop in signal levels because of the loss of power from the line, and it may also generate noise on the line. Direct taps usually require regular maintenance, either to change tapes or replace batteries, which may give away their presence.
- Radio tap - this is like a bug (what's a 'bug') that fits on the telephone line. The state does not normally do this because they have access via the exchange. It can be fitted to one phone inside the house, or outside on the phone line. It may produce noise (you might even get signal feedback down the line on amateur made equipment) to alert you, but probably not. The unit is powered from the line so once installed it's maintenance free, and only transmits when there's a call in progress. However these devices tend to be low powered because the drain on the line would become too great. Therefore the receiver would have to be installed within a few hundred metres of the tap. Radio taps can be found in the same way to line taps, by checking your line regularly.

To guard against unofficial line taps you should know where your telephone line runs, and perhaps inspect it regularly for new joins, or small wires connected to the line.

Location data and mobile phones

Mobile phones are, in surveillance terms, a major liability. This liability will only increase as the new third-generation (3G) phones are introduced. This is because the base stations will be located closer together.

For mobile phones the major threat is the collection of communications data. This data not only includes information about the time and duration of the call, but also the geographical location where the call was made from and to whom. This data can be determined generally because the geographic communications cell that the call was made in is stored with the details of the call. But it is also possible to get greater resolution of a persons location by combining information from a number of cells surrounding the persons location. This additional precision must be specifically enabled by the telephone company - it is not part of ordinary operation. There is no counter-measure against the state/telephone companies doing this.

The old first generation mobile phones could be easily monitored by anyone with a 'scanning all-band receiver' because the system used an analogue transmission system - like an ordinary radio transmitter. The second generation digital phones are harder to monitor because they use a digitally compressed transmission. However the state can tap mobile phones with the co-operation of the phone company. It's also possible for organisations with the correct technical equipment, such as large corporations, to monitor mobile phone communications and decrypt the message. There were proposals for European mobile phones to use stronger encryption, but this was opposed by a number of European states.

Mobile phones can be used anonymously, but it is very expensive to do. Pre-paid mobile phones can be bought without having to give details of your name or address, and because you insert cards there is no

billing information. However, once you have been identified as using a certain phone, you can be tracked. So if you require longer-term anonymity it is necessary to regularly change the phone every few days.

Postal services

As more people use faxes and email the significance of the postal system is decreasing (this may not be the case in all countries, certainly the case with international communications, but probably not local). But interception of post is still very important to the security services.

There is no easy way to know your post is being read. The machines used to sort and stamp letters often rip up items anyway, so damage is no certain indicator that your post is being read.

The simplest counter-measure to stop your post being opened is to put sticky tape along each edge and the seams of the envelope, and then sign the tape with an indelible marker. That prevents all but the most expert tampering.

People used to send floppy disks via the post. Today these files can go easily by email. But CDs of data are still regularly sent by post. To ensure that this data is not open to reading by anyone, even if its just wrongly delivered, you should encrypt the data and then burn it onto the CD-ROM.

Surveillance devices - 'bugs'

Surveillance devices or 'bugs' are not really a communications media, but they are a device that requires a communications channel. The idea of a 'bug' usually involves a radio transmitter, but there are many other options for carrying a signal; you can send radio frequencies through the main wiring of a building and pick them up outside, you can pick up the transmissions from a cordless phones, and you can pick up the data from poorly configured wireless computer networks or tune in to the radio emissions of a computer monitor.

Bugs come in all shapes and sizes. The original purpose of bugs was to relay sound. Today the miniaturisation of electronics has progressed so far then even TV pictures can be broadcast via bugs that incorporate miniature video cameras (something made popular recently during TV coverage sports events, etc.).

Older bugs used the VHF radio band. Modern bugs, thanks to the developments in electronics for mobile phones, work in the UHF and microwave bands. The use of digital rather than analogue technology means that the most professional bugs can encrypt the output signal, and change the frequency of operation in a pseudo-random pattern to make finding them harder. The range of these bugs varies from a few hundred yards to a few miles. Some of the state's bugging devices are even linked to satellite systems. There is a growing commercial market in surveillance devices such as audio and CCTV bugs, mainly for observing people in the workplace. Officially very little of this equipment is used for spying on the activities of pressure groups - but the potential is there.

Amateur bugs are usually the size of a cigarette packet. Professional bugs can fit into pens, calculators and other commonplace items. Some are only the size of small shirt buttons - but the power and operation life of the smallest bugs is very short.

The devices used by persons or organisations without the funding to buy professional equipment are crude. These devices can be bought from electronics magazines, and designs to build them are available on the Internet. They tend to broadcast in or around the VHF frequency band. They are also fairly bulky because they are made from ordinary electrical components and need a conventional battery power supply.

However a well-made amateur bug can be just as effective as a professional one for conducting surveillance.

Another great problem with modern technology is the development of 'wireless' appliances. To be 'wireless' a device must transmit information, either by radio waves or infra-red light, and this potentially makes all the information sent via that link available to others. Radio waves are the worst option, but even infra-red can be picked up through a window. Some wireless devices, such as wireless computer networks, do encrypt transmissions, but the standard forms of encryption are weak.

> *Wireless devices, be it a wireless keyboard or a wireless telephone, should not be used in any environment where sensitive information is handled.*

Bugs emit radio waves. The standard counter-measure for bugs is therefore to 'sweep' for them with a receiver, looking for the radio emissions. Professional sweeping devices are very expensive. There are low-tech sweeping devices available, through amateur electrical magazines, or that can be built from circuit designs on the Internet. But sweeping is not fool proof. Advanced bugs can be remotely operated to switch on and off, and some even rapidly switch frequencies according to a pre-determined pattern in order to make location with sweepers more difficult. You may also be bugged, but you don't detect it when you sweep because it's run out of power.

The other problem are those bugs that do not emit radio waves - they are very difficult to detect. Bugs are a technical solution to a problem - remotely listening to people's conversations. A simpler option is simply to record the conversation on a normal recording machine. There are a number of options for this:

- Pocket sized devices, either worn or carried in baggage, linked to a small microphone that's usually mounted on the surface to pick up the audio. Digital recording devices, such as minidisc or the latest palm-sized camcorders, also give very high quality recordings in a very small device.
- Larger recording devices hidden in the room, for example above suspended ceilings. These are popular in workplaces for monitoring staff.
- Ultra directional microphones. These are like the microphones you see on camcorders, or carried by sound technicians. They are constructed to receive signals only from one direction. The most high-tech directional microphones can eavesdrop on conversations from a hundred metres away or more.
- Laser microphones. These are very expensive and highly technical to operate. You bounce a laser beam of a window, or off some object near the conversation you want to hear that resonates (for example, a picture on a wall). Any object which can resonate/vibrate will do so in response to the pressure waves created by noises present in a room. The electronics detect the minute difference in the distance travelled by the light to pick up this resonance, and reproduce the sound causing that resonance.

If a microphone is hidden in a room it is almost impossible to detect it. This is because it has no radio emission. Very sensitive equipment could be used to look for magnetic fields or electrical noise emanating from the recording equipment. This is because the computerised/digital technology in digital tape recorders emits characteristic electrical noise. But if the place being monitored has lots of computers, photocopiers and other electrical equipment installed that would be very difficult. Older analogue equipment is very difficult to detect.

Computer Surveillance

Computers make excellent surveillance tools because they can do things without their owners knowing about it . At the very basic level, computers are a surveillance tool because you confide your secrets into it.

Anyone can then come along and access or remove your computer and retrieve your information. But if someone is able to install software on your system they can turn your computer into a surveillance device.

Getting software onto a computer can be done in three ways:

- You obtain access to the computer directly - this requires that you load a CD or floppy disk into the computer and transfer the programs. This is possible if someone uses your computer for an innocuous purpose, or they gain access whilst you are not there.
- You can receive a computer virus, form an email or an infected file, that can install a program on your computer. This can enable hackers to gain access to your computer, or it can send information such as your encryption keys to security services (a project the US FBI is currently working on).
- Your computer can be hacked when it is online, and rather than damaging it the hacker can install software on the system that enables them to control it, store information on it, or read your private files. This is more of a problem for Internet servers, but computers with a permanently connected broadband line are also susceptible.

The simplest form of access would be via a new, unique computer virus. This is because it may not be picked up by virus scanning software. It could also use the facilities on your system to compile a digest of the information and usage of your computer, and send that back to its base. Whilst access to your system whilst you are online is possible, it would be difficult to arrange because unless you are online all the time, they will not when precisely when you use the Internet.

To protect against people accessing your computer from the Internet, and also protecting against rogue programs on your computer, you should use a firewall on your network or Internet connection. (refer to Firewalls in briefing 6) This will flag up a warning whenever an unauthorised access takes place. But beware of the Microsoft firewall - it only works on connections going into your computer, so rogue programs can still connect out.

Getting access to your computer is the next most likely. This is a real possibility, since you must assume that the types of people engaged in this kind of surveillance, because of the technical barriers involved, are professionals. They are also likely to have the technical capability to gain access to your home or workplace. You should therefore take steps to limit access to your system.

The briefing on *Introducing Information Security* (no.1) outlines how to protect your information. Perhaps one of the most effective means of preventing opportunistic access, apart from a boot password, is a screen saver with password protection. This is a simple means of preventing access whilst you are away from the computer.

Computer networks are another surveillance problem. Networks operate by sending packets of data to every computer on the network, but only the computer matching the packet address will process that packet of data. Using programs called *packet sniffers* it is possible to read all the packets that cross the network. Using a packet sniffer it is possible for one computer on the system to intercept all data transactions over the system, or just those for one of the other computers. This again could be done using software installed on the system without the knowledge of the computers operator. The problem would be extracting the large volumes of information that sniffing packets can generate. But for only a short period of time, packet sniffing could reveal all sorts of information.

One of the lesser known forms of surveillance goes by the name of 'TEMPEST'. Computer monitors and some other digital equipment emit radio waves as the high-powered coils and transistors switch electricity to create the video image. The same type of emissions can be used by TV companies to detect if their programmes are being watched on an ordinary TV without a license being paid. But with better technology, the actual image on the screen of a computer monitor can be captured and displayed.

One solution to the TEMPEST problem is to use a low powered display, such as a laptop computer. But it is possible that these displays could also emit waves that could be resolved to produce an image. The only certain solution to TEMPEST is to shield a monitor, which is a very difficult thing to do, or specifically buy an extremely expensive shielded monitor.

Finally, computers themselves can be tapped physically. For example, it would be possible to bug the keyboard in a way that transmitted the codes of the keys pressed - in this way it is easy to discover the passwords use to start the computer, as well as the passwords for accessing the Internet, email and encryption keys. Anything beyond tapping the keyboard would require taking your computer apart.

Photography

Photography is becoming more valuable as a means of surveillance. In recent years there has been a significant expansion in the level of stills and video photography carried out at public demonstrations in many countries. At the same time there have been advances in closed circuit television (CCTV) technology and computer image processing that enable digital images taken from cameras to be matched with images stored in a database.

Photographs have long been collected as a form of evidence. But as protest and civil disobedience become an ever greater liability to governments and corporations, images are gathered not only as evidence for prosecution, but also as a source of intelligence information. The collection of photographs and video also has another important function - it scares people.

Closed circuit TV (CCTV) - where the picture is viewed or recorded, but not broadcast - initially developed as a means of security for banks. Today it has developed to the point where it is simple and inexpensive enough to be used in home security systems, and for everyday surveillance.

The widespread use of CCTV by the police and governments has developed over the last 10 years. In the UK, cities and towns across the country have installed large numbers of cameras linked to police authorities. The justification for the growth of CCTV in towns is that it deters crime - although there is still no clear evidence that CCTV reduces crime. The recent growth of CCTV in housing areas also raises serious issues about the extent to which CCTV is being used as a social control measure rather than simply a deterrent to crime.

The first CCTV cameras used in public spaces were crude, low definition black and white systems. Modern CCTV cameras use high definition colour cameras that can not only focus to resolve minute detail, but by linking the control of the cameras to a computer, objects can be tracked semi-automatically. For example, they can track movement across a scene where there should be no movement, or they can lock onto a single object in a busy environment and follow it. Being computerised, this tracking process can also work between cameras.

Currently, in some areas of the UK such as London, CCTV is being combined with computer imaging systems to track car number-plates. This is being developed in part as a security measure, or as a means of identifying cars reported stolen. But there is no reason why a network of such cameras could be used to track the movement of individuals. The proposed road tolling system for London will also rely on reading car number plates to generate billing information - therefore producing a potential source of locational information on persons or groups.

Perhaps the most disturbing extension to this technology is the recognition of faces from high-definition CCTV images. With this technology, it would be possible to determine a person's identity without the need to stop and ask them in the street, or even alert them that their identity is being checked and logged. The systems can check many thousands of faces in a database in under a second.

The latest developments in CCTV and imaging techniques, being developed in the UK and USA, is developing computerised monitoring so that the CCTV operator does not have to endlessly look at all the screens. This also means that an operator can run many more CCTV cameras. These systems do not observe people directly. Instead they track their behaviour by looking for particular types of movement, or particular types of clothing or baggage. In public spaces people behave in set and predictable ways. People who are not part of the 'crowd', for example car thieves, do not behave in the same way. The computer can identify their movements, and alert the operator that they are acting out of the ordinary. Potentially, waiting in a busy street to meet someone could trigger this system.

The same type of system can, if required, go one step further and track an identified individual as they move through the area covered by CCTV. This is currently being developed in the USA as part of the project co-funded by the US Defense Advanced Research Projects Agency. With software tools, the system will be able to develop three-dimensional models of an area and track/monitor the movement of objects within it.

The development of CCTV in public areas, linked to computer databases of people's pictures and identity, presents a serious risk to civil liberties. Potentially you will not be able to meet anonymously in a public place. You will not be able to drive or walk anonymously around a city. Demonstrations or assemblies in public places could be affected as the state would be able to collate lists of those leading them, taking part, or even just talking with protesters in the street.

Documentation trails

Modern society creates huge amounts of data. Every time you use a bank machine, pay by credit card, use a phone card or make a call from home you clock up electronic records of transactions. In the past these would have been called 'paper trails'. But today many of these records are electronic. This information, if obtained by the state, or obtained through unofficial channels (sorting your rubbish/bribing those in charge of keeping the information) can also describe how you live and work.

The scope of the information that can be obtained from paper trails is growing all the time as our lives become more monitored. Once many sources of information are matched as part of intelligence analysis it can produce an insight into your habits, your work, and your hobbies.

The abolition of cash, and the introduction of 'electronic money', could be one of the greatest blows to free expression and free association in modern times. As we move towards the 'cash-less society', all electronic transactions will have to be monitored at an even more intensive rate in to prevent electronic forgery. There will have to be detailed records of every transaction, and the two parties involved in that transaction (e.g., you and a shop), in order that every credit and debit can be matched up to ensure that no extra money was plugged into the system. Of course, this will mean that, unless you barter outside of the mainstream system, all transactions will be traceable by the state, and possibly even large corporations.

One of the greatest freedoms we have is to buy a book, or a newspaper, or to donate money to a cause, and do so with complete anonymity. In a situation where all transactions are electronic, and the information about all transactions must be audited to prevent fraud, that anonymity is lost.

However, the primary problem relating to the use of documents and data is not the state. Compared to how marketing and PR companies assemble data on individuals, the security services could be considered mere beginners. Today a whole web of information is collected by marketing companies in order to sell you things, or determine how companies should run their marketing strategies. Many people unwittingly assist in this. Today you don't have to fill in a survey form to be besieged with junk mail. The details from a whole range of transactions, from credit agreements to the electoral register, are all purchased by market research companies to provide information on the habits of the public as potential customers.

Data profiling

Most of the information described above is generalised - it identifies trends from large quantities of data, and the role of the individual in that is very minor. *Data profiling* on the other hand is a process whereby someone seeks to get as much information about you as possible - *personally* - in order to assemble a picture of your specific life and habits.

Data profiling is very important in intelligence operations and has many applications - from deciding whether a person is vulnerable to bribery, through to conducting profiling of suspects to decide where they can be apprehended. The state has powers to do this by issuing orders that banks, credit companies or even your employer supply data to them. But even corporations and private investigators can assemble this information if they are well connected. The problem is that a lot of your personal information is not very well protected. This is because, in isolation, small amounts of information is not considered sensitive. But once this information is brought together it can describe in detail the actions, habits and preferences of the individual.

Identities

Identity is an important issue in terms of civil liberties. There are instances when we wish to hide our identity - to remain anonymous - for a whole range of reasons. To eliminate this will be a serious erosion of our civil liberties. This is possible as we move towards the development of 'electronic identities. There are two aspects to this:

- the development of systems of credentials - where you carry a card or a document; and
- the development of biometrics - where you are recognised from your 'unique' biological characteristics.

The development of identity systems is being pushed on two fronts:

- The banking industry - who wish to find a more fool proof system of verifying financial transactions than the possession of a plastic card or the use of a signature;
- Law enforcement - who want a way of identifying individuals easily, perhaps even when they are unwilling to co-operate.

One of the simplest forms of identification is the carrying of credentials. Some countries have an identity card system to aid identification. Other documents, such as drivers licenses, library cards, bankers or credit cards are also used to verify identity. The problem with identity based on credentials is that the individual must carry them, and be identifiable, or face a legal penalty. This problem is compounded if the form of the identify card is 'machine-readable' (could you explain more) In this case it may create a document trail as it is used to verify transactions.

As a means of combating the problem of people carrying or falsifying credentials, researchers are increasingly looking at biometrics - measuring biological or physical characteristics - as a way to determine identity. One of the oldest forms of biometrics is fingerprints. Everyone (identical siblings excepted) has a unique pattern of fingerprints, and these have been used for many years to help identify suspects in police enquiries. A finger/thumb print can be reduced to a brief numeric description, and such systems are being used in banks and secure areas to verify identity.
A more recent development is DNA fingerprinting, which looks at some of the major markers in the body's DNA to produce a match. However, the match produced is less accurate than ordinary fingerprints because it only identifies people to within one family - not the individual themselves.

Handwriting - primarily your signature - has been used for many years to determine identity. However other

characteristics of the individual can also be used to check identity. Voice analysis has been used for some as a means to prove identity - but it is not suited to portable use because of the problems of storing a range of voice prints. But perhaps the two most viable portable systems, because identities can be reduced to a series of numeric data points rather than a detailed image or sound, are:

- *Iris recognition*. Some banks are now using this method of security. The human iris has an almost unique pattern that can be reduced to a simple series of numeric descriptions. The iris reader matches the pattern of the iris to one stored and verifies the match.
- *Facial recognition.* The configuration of the facial features can be used to accurately identify one individual from another. Again, the configuration can be reduced to a short numeric description.

By combining some form of personal identifying feature, with a system of verification it is possible to do everything from buying food to travelling abroad. The important issue is how this information is managed in order to reduce the likelihood of tracking. If you were to combine a particular biometric system with new smart card technology to store the description, that system would be immune from tracking (unless the transaction produced a document/electronic trial). But if the identifying features are stored centrally, and a whole range of systems have access to those descriptions, it is possible that other uses could be made of the data; for example, using high resolution CCTV images with a databases of facial identities in order to identify people at random.

Human operatives and social engineering

The most invasive form of surveillance is the use of human operatives. This takes two forms:

- The use of operatives to infiltrate an organisation; and
- The use of social engineering techniques to obtain information.

In groups dealing with issues that are directly contrary to government policy the issue of infiltration often arises. Also, where groups oppose large corporations, infiltration by agents of the corporation is also feared. As well as operatives, the police and security services may put pressure on certain members of an organisation to disclose the information they hold on other members.

Running operatives is very expensive, and for the state the information recovered from operatives can be obtained from less problematic forms of surveillance. If discovered, it can also be a public relations disaster for the government or corporation involved. For these reasons, the use of operatives to infiltrate organisations is not as widespread as many believe. But infiltration is still very likely from other organisations who are motivated to discover and monitor the work of campaign groups. This may be for political or economic motivations. There are also many informal links between large corporations and police or security services, and the trading of information about groups and activists is part of this relationship.

It is not possible to guard against the infiltration of an organisation without damaging the viability or effectiveness of the organisation. Worrying too much about infiltration within the organisation can breed mistrust and bad working relationships within an organisation. Rather like other forms of surveillance, the professional infiltration of operatives into and organisation is difficult to guard against.

Another more likely scenario, especially when dealing with the media or corporate public relations, is social engineering. Social engineering is where someone phones you, interviews you, or just talks to you in the street and tries to make you believe they are someone else, or someone with an innocuous interest in you. But their real interest is to obtain some specific information that they believe you possess.

You should develop clear procedures for handling enquiries about your work. For example, one day you get a phone call saying "hi, I'd really like to come on your demonstration against Company X, when is it?", or, "I'm calling for john, he's lost the password for the computer can you give it to me?". You have to guard against the disclosure of information in this way:

Unless you have an extremely good reason to, you should never give any security-related information over the phone, and via the Internet you should encrypt security information.

Social engineering is easily identified by asking a series a questions to see if a person is aware of facts or future plans that they should not have awareness of.

Journalists are a particular problem. Journalists for well known media organisation can be verified by phoning the editor of that organisation, but freelance or independent journalists should be treated with care - they could be working for anyone.

There is of course a balance to be struck here. You need to be able to allow people a certain amount of access to your campaigns. But you also need to preserve the integrity of the groups of people most closely involved in the campaigns work. How you arrive at this balance is your own, difficult, problem to resolve. But however it is resolved, it must be agreed between all those involved in a particular issue in order that you have a consistent policy with all those involved.

Personal counter-surveillance

Counter-surveillance is reliant on good information security planning. The briefing on *Introducing Information Security* (no.1) outlines how to protect your information - including information on counter-surveillance in the workplace. Protecting information is the first stage of counter-surveillance. But counter surveillance must also be seen as a balancing of opposing objectives.

If you are very good at restricting all information, that state or corporations will have problems monitoring you. However, you are also likely to become more isolated and secretive in the process, which may isolate you from the public you are trying to engage. Therefore, like information security, counter surveillance requires an effort to protect those activities or information that are sensitive, whilst giving less emphasis to those activities that can be open to all.

Information security is primarily based on protecting equipment with security procedures and barriers. Personal counter-surveillance is based on much the same process, but instead you provide security and barriers around your own personal habits. As humans we are creatures of habit. If we exhibit very predictable habits. This makes monitoring of our activities easier. But if on certain occasions we break our habits, it can also give away the fact that we are doing something at that time which is not part of our everyday work.

The best way to begin thinking about avoiding surveillance is to think about breaking the regular patterns in your life. This masks regular activity, so making it harder to practice routine surveillance. But it also masks the times when you may undertake activities out of the ordinary.

Breaking regular patterns does not mean going to bed at different times, or working different hours everyday. Instead it requires that any activities you wish to avoid being the subject of surveillance are integrated into the other events in your life - but not to the extent that they become predictable. If you change the route you take to work or to shop on a random basis, you make it more difficult to monitor your movements. If you build irregular appointments into activities that might involve surveillance, it creates a background 'noise' in the pattern of your activities that masks any change in your habits.

Securing the information on your computer will help your overall security. If you have a portable computer

you are presented with a whole new problem because you move that system outside of your ordinary systems of security and access barriers. Therefore special care should be taken with portable computers:

- The system should be secured with a BIOS password to prevent booting;
- Use encryption of the hard disk, where possible, to prevent access to the contents of the hard disk if it is removed from the machine;
- You should ensure that your portable computer has different passwords than those used on your static equipment.

Securing your information is fairly easy. But the main issue you will have to deal with when considering personal surveillance is how to carry out meetings, and networking with people, when you need to discuss sensitive issues.

You should not seek to avoid surveillance for issues that have no sensitivity. This of course assumes that sensitive work only constitutes a minor part of your work. Where the sensitive parts of your work comprise a large part of your everyday workload the more difficult it will be to hide those activities within the patterns of your everyday life.

Primarily, when dealing with sensitive information, you should avoid generating any kind of documentation or opportunities for surveillance by working systematically to avoid it. As society becomes more highly surveilled, this is becoming more difficult to do. As governments begin to use communications and transactions data as an increasingly significant part of their effort to monitor the activities of their citizens, you should work in a way that does not generate systematic document trails. To do this, you should think about implementing the following as part of your work:

Travel -

- If you are travelling to a sensitive meeting take a different route going there and coming back, and if possible do not use the same bus or station when going to or leaving the location you are travelling to. This lessens the likelihood that your destination will be identified.
- If travelling on sensitive business, try to use public transport. Using you own private cars will provide a traceable identity.
- To avoid the CCTV systems in public places move with the crowd; don't rush, don't cut corners, and don't look around for CCTV cameras.
- If you can build in other events/appointments as part of your journey, that will help provide an alternate motive for travelling to that area of a town or city.
- Facial recognition systems work primarily on the configuration of facial features. To work they need to get a good view of the face. Looking at a slight angle towards the ground, and wearing a hat with a brim, helps fool the system.
- If you travel using public transport, roaming tickets are preferable to tickets for a specific journey - they give you more flexibility over the route, and they are more difficult to associate a route travelled with a particular ticket purchase.
- If you have the time available and you can obtain a roaming ticket, build in some extra time to your journey and change trains to make it hard to piece together your journey from CCTV and surveillance sources.
- If travelling in a town, avoid moving through the major shopping areas, or 'controlled environments' such as shopping centres. These have the highest level of CCTV coverage.
- Always assume that public transport vehicles have CCTV installed - travelling during peak hours will help mask your presence.
- To make following you in person or via CCTV more difficult do not wear distinctive clothes or carry distinctive objects - blend in.

- Darkness aids anonymity, but is not a foolproof solution to the latest CCTV cameras which can see in the dark.

Mobile phones -

- If in doubt, turn it off.
- If travelling to a sensitive location, in an urban area do not use your phone within two or three miles of the location, or in rural areas do not use it within ten or fifteen miles of the location. This will prevent the creation of a trail that associates you with that location on that day.
- If the location you are going to is nowhere near a route you regularly travel, turn off your phone before you start your journey there.
- If you desperately need to mask your location, let someone else carry your phone around for the day - but this is only realistic if you take all precautions to prevent generating other document trails whilst you are moving around.

Payments -

- If you are travelling to a sensitive location, don't pay by credit/debit card or take money from a cash machine.
- If you need to spend cash when travelling to/working around a sensitive location, do not spend the notes taken directly from the cash machine (their sequential numbers may be logged). Keep a supply of notes received as change elsewhere and use those.
- If you need to buy something when travelling to/working around a sensitive location, do not give any loyalty cards or personalised money off tokens as part of your purchases - they are traceable.

Communications -

- If you need to make a sensitive phone call that must not be directly associated with you, do so from a public phone box. But beware, if you are associated with the person at the other end of the call, and the content of their calls (rather than just the data) is being monitored, your location at that date and time will be discovered.
- If using public phone boxes, try to use them randomly across an area rather than the ones that are closest to you. Also, try to avoid phone boxes on direct transport routes to your home or place of work.
- If you wish to send something sensitive through the post, wear gloves to prevent creating fingerprints when producing/packing the item, do not lick the envelope or stamps to prevent creating a DNA sample, and post it in a different location to where you normally post your letters (the further the better) using stamps bought on a different day.
- If you need to send a sensitive fax, use a copy shop/bureau which has a self-service desk.
- If you desperately need to keep in communication, buy a pay-as-you-go mobile phone and only use it for a day or two whilst you are engaged in sensitive work.

Online -

- Maintain a number of alternate personas (see briefing no.6 on Using the Internet Securely) on the Internet that give you access to web mail and other services should you ever need to use them.
- If you need to use the Internet, use a cybercafe, but make sure that you do not access your own Internet services from the cybercafe - use an alternate persona.
- If you need to view material that you do not wish to be associated with as part of the server logs of your Internet service provider, use a cybercafe.

- If you use cybercafes as part of your communications, try not to use the same one.
- If you have a laptop computer, and you wish to mask your location, let someone you trust use it online whilst you are away on sensitive work.

Meetings -

- When organising a private meeting, if you cannot send details to all involved in ways that will not be intercepted always try to agree on meeting in one location near to the meeting place. You can then direct people to the correct location as they arrive. By keeping the location of a private meeting limited, you lessen the likelihood of the location being surveilled.
- If meeting in the home or building of another person or organisation do not make a phone call from their phone to a number that is identified with you, or from a public phone box near to that building.
- If the people going to a private meeting are likely to have mobile phones, ask them to turn them off before travelling to the meeting place (if all the mobile phones of a groups of people are in the same cell at the same time on the same day, it can be assumed that you have had a meeting).
- If you require a private meeting place, do not keep using the same one. Alternate it as much as possible. Also, if you meet in a public place, pick somewhere with a high level of background noise, and with as many obstacles or partitions around the point where you meet, to prevent your conversations being overheard.
- If you must pay for something whilst having a meeting, use cash. Or, if you cannot, get one person to pay. In this way you will not generate paper trails linking you together.
- Meeting in public spaces, streets, in parks, or on public transport is not a good idea - many of these areas are surveilled by CCTV. But bars, cafes and restaurants tend not have their CCTV systems linked to a central control room, and what CCTV systems are installed are concentrated around the till.

In conclusion...

There is not foolproof formula for counter surveillance. If the state directs all of its resources to monitoring your every move, they will be able to do so. But as members of a society working to change the organisation of that society peacefully, it is not likely that we will be subjected to the highest levels of state surveillance. Therefore we're not looking to defeat the high-tech, high-cost types of surveillance. We're looking to control our exposure to the everyday types of passive surveillance practised by the state, and the opportunistic actions of corporations who are interested in our activities.

The important rule with counter surveillance is proportionality. Seeking to prevent all surveillance would mark us out as so deviant compared to all other members of society that it would actually attract attention. Instead it important to apply a level of counter surveillance in proportion to the sensitivity of the information or action involved. In this way we prevent our actions being so deviant in their patterns from the norm of society as a whole. In this way the work we wish to protect should slip through un-noticed.

The final issue with counter surveillance is one of justification. We must be able, if challenged, to justify our use of counter surveillance techniques. Otherwise our use of these tactics could be used by the state or security services as evidence of guilt in the conduct of our activities.

We are guaranteed, under human rights conventions, rights to free expression, association and conscience. These rights can only be exercised where we have the ability to interact with others in a way which is not subject to routine surveillance. Today, thanks to digital technology, surveillance has become so pervasive that reaching an environment where it is possible to exercise human rights free from state or private intervention is very difficult. Human rights are subjective. This means that the human rights of

someone engaged in social change are interpreted differently from the rights of someone who engages in organising local sporting activities. For those engaged in legitimate and otherwise 'public' social change and protest activity, and who believe that their work is unwelcomed by corporations or the state, counter surveillance is a legitimate part of their work in order to exercise their human rights.