..::www. A c t i v i s t S e c u r i t y .org::..

A Practical Security Handbook for Activists and Campaigns (v 2.7)

This guide is dedicated to all those who have died for freedom. Many have been honoured; many, many more have no one to recall their sacrifice. It does not take much to be a hero, just to stand up in the face of injustice, when the odds are overwhelming, and stand firm for what you believe in. We honour them through our own actions to preserve the liberties of others.

" The price of freedom is eternal vigilance"
Wendell Phillips or Thomas Jefferson

Disclaimer: everything in this handbook is for information purposes only. Please do not use it to do anything illegal, but protect your right to protest and change the world for a better place. We cannot take responsibility for your actions, though we say that you should be as active as possible.

First Published October 2004.
Version 2.7 published June 2008

1. Introduction

This booklet is an introduction to security for action and activists. It is hoped it will provide you with the necessary information for taking action and for effective campaigning in the face of state and corporate oppression.

The authors are activists who have been taking direct action and campaigning on a variety of issues for many years. In that time they have encountered the state and various opponents on a number of different levels and survived to tell the tale (for the most part). It is a summation of our experience in the hope that it helps you avoid some of our mistakes.

Much of the material in this book is common sense. There is a lot of information contained in it but it should be fairly obvious for the most part. You will not need all of it, but you should find the information to deal with any situation you may be in or planning for. In places we have been repetitious so that each chapter is able to stand as much as possible on its own, though we urge you to read all of this chapter – like most actions and campaigns, the philosophical groundwork is vital.

The approach we recommend is to first work out what sort of threat you feel you are facing and learn accordingly. If you do not need to worry about stuff because you are not active in a particular direction, then do not stress about it. It is better to be clear about what you are doing than trying to be everything.

If you have new information or we have made mistakes then please let us know at handbook@activistsecurity.org so we can update the next version. This is vital as wrong information can bring about to a false sense of security which in turn leads to actions and campaigns being compromised.

1.1 Why security is important

Security is important as we live in a world where upsetting the status quo to change the world for the better is generally met by a backlash. Governments, law enforcement agencies and corporations all have vested interests in criminalizing, disrupting and suppressing activist groups of all persuasions. Security is needed to ensure our continued success. We also have a basic right to protect your privacy and anonymity from unwarranted intrusion.

For those who say that we shouldn't have anything to hide or should make a principled stand on it, well we live in a world where democracy is subverted daily and the people doing it the most are those in power. As long as governments and their supporting apparatus permit corruption through their closed and secretive natures then we need to respond in kind for our own protection.

Threats do not just come from the state. There are situations were media organisations with their own agenda will attempt to target campaign groups. Private investigators also need to be factored in as threats. Both have distinct issues which also need to be dealt with to ensure your message successfully gets to the public without being intercepted or disrupted.

1.2 What is security?

Everybody has their own ideas of what security is, and indeed security is a very individual issue. Different people have different needs, and no one solution fits all. What works for someone else may not work for you. However, there are certain fundamentals that apply to all situations.

Security is a *process* that protects you in some fashion, whether in the run up to, during or after the event(s) you are involved in. This means, that security is there to *facilitate* the smooth operation of your action, campaign, etc. and help keep everyone safe.

A common mistake is equating paranoia with security. Paranoia is often used as an excuse not to take action through fear of what can go wrong – normally by over-stating the omnipotence of opponents. In our experience paranoid people have little to fear as they are too nervous to do anything that would actually put them at risk. Indeed, few even have security measures put in place. This sort of fear means you effectively defeat yourself.

There is no such thing as a 100% fail-safe system, and not doing actions because you cannot reach that level of security is not an excuse for copping out. There is always some risk; and security processes help reduce that risk to an acceptable level. It is up to you to define what the acceptable level of risk is and how best you can deal with it. Sometimes you just have to take a chance.

Security is not a single thing; it is a *process* and a *state of mind*. You cannot put down and pick up security at whim. For security to be effective and worth the time and effort put into it, it has to be built into your life. Ideally, it becomes second nature; that is, you automatically go through the processes that keep you secure. This creates a mindset that helps you avoid errors of judgement you may regret later. There are objects and software that will aid your security, but simply having them is not security in itself; they need to be are part of an active security process. For example, there is no point having a bug scanner if you don't use it on a regular basis. Likewise anti-virus software will not protect your computer unless it updated regularly.

There are many levels to security, but it needs to be built into your life/campaign/action right from the start. Picking it up half way through or after an action is generally too late. Hence, when you start planning, think about the situation and the threats that may arise, so you are incorporating features that protect your security as you go along. It makes protecting yourself far easier and means you are less likely to make mistakes.

The most important lesson when it comes to security is the equation:

Security = Time + Effort

You cannot get around this basic fact; every security measure will have some sort of impact on your life, including work. Security requires you to be pro-active and to put the effort in. And you need to be prepared for this. Once you have decided on the appropriate security process, there is no room for shortcuts. Shortcuts are gaping holes in your plan that end up compromising you. Yes, there are times when you are just too tired to encrypt all your sensitive files, but what is that one half hour compared to the prison sentence which may await you should you get raided the following morning?

Finally, if you are part of a group, security is not just about yourself, but about everyone you are involved with. Slackness on your part means are you compromising them, and you do have a responsibility to them. If you are making mistakes which allow your opponents to find out crucial and sensitive data on your colleagues then you are effectively betraying them. Not a comfortable thought, but an important one.

1.3 Setting up the 'Security Process'

We noted above that security is a process to be built in from the start. The best approach is to decide what it is you want to achieve, make plans and then identify the points where you could be compromised. Once you have done this, work out security tactics to stop those potential compromises from becoming unacceptable risks.

As a simple example, writing an anonymous letter – you don't want to leave fingerprints on it, so the security process is to wear gloves when ever handling the paper and envelope. You are not making yourself paranoid over the fact that they might find your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your action of writing the letter securely.

Using gloves to write a letter is clumsy and awkward so slows the whole process; however if you do not put in this extra time and effort then it is possible the letter could be traced back to you, and depending on the contents it could mean you losing a lot more time…

On a practical level for campaigners and activists most security processes are essentially about controlling the flow of information about yourself and your plans, whether electronic, personal data, paper trails or physical evidence which connects you to the action. Later we will discuss the specifics of what these can be and what to do about them. When you understand where there are potentially betraying information leaks out, you arrange to have the security techniques and processes to stem that flow, or at least make it very difficult for it to be traced.

A security process is either a course of action or a technique adapted to your needs and situation.

Keep in mind that the state/corporations are not all powerful though it may appear so (they encourage this belief themselves). They are restricted by budgets and simple manpower, or even infighting. They also have poor understanding about how activist groups work, and just because one part of the organisation has a good picture of your set-up or access to the latest equipment, it does not mean that it is true of the rest.

There are a number of groups that have managed to be very active and sustained that level of activity in the face of intense pressure. They have achieved this by having security built into everything they do, possibly to a higher level of security than actually needed. This has the advantage that it makes it much harder for them to be penetrated, and any mistakes which occur do not have the drastic impact they could otherwise. Their level of security is not going to suit everyone; many campaigners will not have the same sort of pressure and unless you are ready to deal with the sort of effort which accompanies it, it may not aid you at all. It is better to find a level you are comfortable with and able to work with in than strive to be more secure than is necessary so end up squandering your resources on security at the expense of being active.

Although it is better to overestimate than underestimate those we are taking on, do not fall into the trap of believing their hype. It is a common trick to send out disinformation about the technological and resources at their disposal. The reality is a lot of the hype fails to materialise or the techniques are easily defeated. Another tactic is to make out they have infiltrators and grasses when they don't. Bear all this in mind when working out your security needs; some of the threats will be real, but not every one. At the end of the day, what is more important is what the state and others use on a practical level in day-to-day work and not so much the theoretical powers available to them.

A common mistake activists make is to believe that when they are being investigated it is to catch them for a crime. This is often not the case. People come under scrutiny as security agencies spend a lot of time and effort on building up profiles of who is networking and friends with whom. This is actually planning their behalf as it means when something does happen they have better idea of where to go looking. These information networks are vital to their intelligence and profiling, and the easily built up through simple things as who is phoning who.

Fortunately for us, their resources are rarely up for more than cursory work unless a political decision is made to focus on a group in particular. The less you can show your head above the parapet and attract attention to yourself the better. An example of this which we will cover later is all the photographing at demos – they are not taking photos of you but who you are talking to or have travelled with.

Mistakes happen, even to experienced activists. It is a fact of life, especially when doing actions under stressful situations. This is why it is best not to do sensitive stuff when tired. A mistake is not an excuse to down tools. If your security process is set up right, it should be able to tolerate mistakes and work around them. This is not to say that there are not some mistakes that can completely jeopardise an action, but not every mistake is in this category, and you should recognise the difference.
If someone makes a mistake, let them know but don't treat them as a pariah on the basis of one; the time to get concerned is when mistakes are being made repetitively and they are not making an effort to learn from them, even when it is pointed out.

Review your security regularly. What has changed in a) your life / campaign, and b) in terms of their abilities or focus? If there are changes what do you need to adjust? The world of surveillance is a changing one, if not particularly fast. However, it is too easy to get complacent and assume everything is fine. Return to the issue and give it consideration every few months to make sure you are remaining one step ahead.

Finally, sit down and take time to plan your security needs and how they will impact on your life and your activity. Besides a willingness to take the time and effort to achieve good security, good planning is vital. It goes a long way to help you implement a secure system as well as understanding and (more importantly) dealing with the risks and weaknesses better.

As we have noted several times, security is there to facilitate your campaign or action. It is not an end in itself. So remember not to loose sight of who you are. Plan your security around your campaigning needs, integrating both, and don't let your security define what you do or who you are.

1.4 Other resources

There are not many resources out there, though we have put links to websites in parts of the text to back up what we are saying. However, there are three that do come recommend-

Eveline Lubber's book "**Battling Big Business: Countering Greenwash Front Groups and Other Forms of Corporate Deception"** (ISBN: 978-1903998144) is a clear account of various attempts by corporations to counter the campaigns against them, including the dirty tricks and covert actions they used. Somewhat dated in terms of technological advances, it is still a great insight into how the companies think, and low tech approaches both by the companies and the campaigns. It also has many useful casebook accounts of strategies used to by campaigns to defend themselves against attack by corporations.

Protection International's manual is the only other online security handbook we know of. It has a particular focus (ie. working in countries freer about the use of repressive force against dissident groups) and differing political direction from us, but we feel it complements our work and is great for providing checklists of what to do. It is somewhat short on practical details in places but think we have filled most of the gaps. Well worth a read. Find it at http://www.protectionline.org/The-manual.html

The Register online newspaper has many stories covering computer security, hi-tech surveillance and miscellaneous privacy issues. Free online at http://www.theregister.co.uk. Has an irreverent approach and generally cynical about governments. For more in depth analyses check out Bruce Schneier's "Crypto-Gram" newsletter; which regularly covers a much wider range of security related issues than cryptography, in highly informative essays. See http://www.schneier.com/crypto-gram.html

Finally, in terms of the many tactics of surveillance used by police forces and private investigators alike check out Peter Jenkins author of several excellent manuals on the techniques used and which can be brought from most online booksellers.

2. Security for Campaigns

The fact you are involved in a campaign which aiming to change the *status quo* in some fashion means you are a threat to someone in some fashion. There is no telling how your opposition will react, and some do out of all proportion to what it is you are actually trying to do. Security for campaigns is not just about protecting the campaigners from harassment but also protecting the campaign tactics and preventing smear campaigns and disruption.

When thinking about the security processes you need in place for your campaign, draw up a list of all threats that you may face: state, private investigators, media, your opposition, internal issues and what they can do against you. Often people tend to focus just on the threat from a politically motivated police, but these are not just the only risks (think media exposes, etc.). However, most of the techniques dealing with the various threats are complementary.

That the principle threat is often the state has lead people to focus on the 'criminal law' side of things; but this is only part of the picture. Other tactics used against campaigns are civil injunctions and disruption, and what feeds these is information about internal structure and problems. If the opposition can draw up a detailed picture of who does what and how each individual relates to each other then it make it much easier for the campaign to be infiltrated and disrupted. Resources will then be directed at your mist vulnerable points and key personnel, Disruption can either be anticipating your campaigns tactics so effectively countering them and undoing all your hard work, or else causing splits within the group. It can also involve the arrests of key activists, theft/damage of equipment and smear campaigns.

The ultimate goal is not necessarily to shut you down but to make you ineffective.

2.1 Basic campaign security

Basic security is thinking about where you are leaking information. This is where you let out information about yourself to the public, the media and to other activists, all of which can be used to build a picture about you.

Below are suggestions on what you can do as a campaign to protect yourself. Security is not just about protecting your people or information, but also the campaign's reputation as that is also targeted. It is much harder to promote your message if you have been successfully discredited or been pre-empted.

As a campaign, you need to discuss security in a dedicated meeting and reach a consensus on it. Dictating security only breeds an attitude whereby people not happy with the person making the requests and end up not fully complying with the demands. All campaigners in the group need to understand that there is a need for security measures even if they do not have access to all the information why. Open discussion helps brings up issues, misunderstandings and also build trust. People who feel included in the process are more likely to stick to it – and no amount of formal polices will not protect you from fellow campaigners feeling at odds with them.

It is also important to ensure new or temporary volunteers are also brought up too speed, before they start working for you, not half way through. Never be patronizing about security; explain why it is needed – practical examples always work well. Show people that security can be part of the empowerment process and not just a meaningless chore they are being forced to go through. Cooperation is the keyword here.

a) ***Media Strategy***:

a)a. It is best to have an experienced person dedicated to handling the media. They will have a better sense if the call is genuine and will be better able to deal with the tricks of an interviewer with an agenda which may catch out an inexperienced person or someone new to a campaign.

a)b. Have a pseudonym ready to use. You are not required to give your own name. However, it is better to be ready for this and prepare a name so it is on the tip of your tongue when the media ring up. If you suddenly decide to use a false name then the chances are you will end up stumbling over it, so sounding suspicious. Use the false name for a while and then change it. It is a good idea to change both fist and second names otherwise you just end up being known by the pseudonym, which defeats its purpose.

If asked where an old pseudonym has gone, say that they've left for another campaign, or out of the office.

Press releases can be treated the same way. Consider sowing disinformation by using false names and positions.

a)c. Be ready for contentious issues. Watch out for barbed questions in the middle of long interviews especially on the background of individuals or direct action. No matter how fluffy you portray yourself as, journalists will always dig for 'juicier' bits of information. Be prepared so you will not be caught out and end up saying things you will regret later. You also come across as being professional.

a)d. Do not meet press at your office or home – there is no need for them to get a "feel" for your campaign in this fashion, as you actions and statements should speak for themselves.

a)e. Be wary of requests to meet other campaigners, especially "direct activists"; say you need to consult with them first and will get back to them on that point, but don't make promises. The media are interested in a juicy story and you cannot trust their promises of fair reporting or of putting your side of the story. Do not follow the media's agenda – stick your own.

a)f. The media is a classic method of infiltration. If you are approached by a media organisation asking for more than a straight forward interview, find out all you can about them first. Check out their existence and what other projects they have been involved in, or get the details of other people they have worked with.

a)f.i. In one case, an activist was approached to be interview in a film at home by some journalists who gave good credentials. However, on ask around and doing an investigation of the other they claimed to have been involved in it was discovered that they were right-wingers with a history of fitting up activists.

a)f.ii. In a more extreme case, a film company approached a campaign wanting to do a documentary on its activists. The campaign was naturally cagey but saw the benefits of such a documentary. They met a few times with the journalist, even allowing for the fact that the he seemed to be conveniently on the way elsewhere so him turning up in the town where the office was based did seem to check out. An activist did agree to meet with him in London where the journalist was based, getting as far as the door to the Oxford Street building where the company was alleged to be based (and there was indeed the correct company above the bell).

Suspicions were raised over the professionalism and camera work of the journalist and contact was severed politely. However, on checking it turned out that no such company existed, or were there any other media companies at that address, and no reports in the journalists name came to light, including searches in specialist publications.

Much of this could have been avoided by demanding more details up front and checking them out, not just going on the numbers or claims the journalist provided. It probably would have ended sooner if the activist in London had insisted on actually visiting the office itself instead of waiting outside.

Note that suspicions were raised for other reasons not mentioned here, and this is not a tale for suspecting all journalists. However, when dealing with requests to meet 'frontline activists' or meetings in your office it pays to do at least a little research.

b) ***Your address*** – why make it easy to find you when you can get a PO Box. Not so well known is that anyone can ring up the post office and find to whom it is registered, including addresses. A stronger, if more expensive solution, is to get a mail drop box. There are several firms which offer such services and who will not give the information out unless there is a warrant. The one we recommend for the UK is British Monomarks (www.britishmonomarks.co.uk) who have a better reputation for protecting their customers' privacy and dealing with activist groups in general.

c) ***Answering emails, letters and phone calls***. As with the media, why use your real name. Letters and emails can all be stored, and phone calls taped by those on the other end, though in theory they should inform you.

c)a. When answering the phone give the group name as oppose to you personal name.
c)b. If you are posting on newsgroups, writing letters, etc use a generic email account that is not traceable to anyone in particular, or else an account that gives a fake name.
c)c. Create a fake persona to go with the fake name, in case people ring up asking for them. However, it is best to change the name every few months.
c)d. Ideally, though it can get confusing, consider using different names for different functions, eg merchandizing, webmasters, etc.
c)e. Do not give out the names of co-workers, rather refer them to by position/title.
c)f. On no account should you give out home or mobile numbers of someone else without their express permission. We would similarly advise you do the same for yourself.

If you are suspicious of a caller ask them for a name, company, department and a number or email you can ring them back on. This will deal with most bogus callers. Pretences you can use are

h. You are just a secretary so do not have access to that information
i. The information is not to hand and you will have to go to another room
j. The relevant person with the knowledge is not currently around.

k. Ask them to put the questions in writing or in an email (also gives you address/email details which can be used to confirm authenticity of the caller). Few things are that urgent that they cannot wait the time it takes to do this, and on closer inspection most details are not the sort that are absolutely necessary for a journalists story to be printed.

You can also search to check if they company is genuine and that the number matches up. Some will actually use details from real companies to give authenticity, which is why you should also ring the company switchboard to check that they are genuine employees – ask to be put through to their office, as opposed to asking straight out if they actually work there. One advantage here is that it may give you a chance to listen to their voicemail so checking if their voices do actually match up.

This also applies to dealing with media requests, or phone calls from other activist organisations. Don't be offended if someone doesn't trust you straight way over the phone – it is a basic and important security principle for who is to say you are actually who you claim to be.

Questions to be immediately wary of are those asking for organisational or structural details. Often it is the innocuous details they are looking for, buried in among other questions so you do not realise what they are after. Social engineers who specialise in this sort of investigative work never ask for the details they are interested in straight out but work the conversation so that you volunteer it of their own accord. For example, they may assume a fact in their question, appearing more knowledgeable than they are, so when answering the question you are inadvertently confirming the fact, the real target of their inquiry. One book worth reading to see practical examples of how social engineers and private investigators use innocuous details about the organisation to find more sensitive information is "*The Art of Deception*" by Kevin D Mitnick.

All this is irrelevant if your volunteers are not also briefed on organisation policy, so this is a very important point to cover with them. It is a mistake to think that only certain or senior people in an organisation are going to be the target of social engineering attacks; rather junior/new people are just as likely to be targeted as they may not appreciate the full value of the information they are giving out, or the same instinctive feeling for a suspect call.

If you take one point away from this subsection it is: *if in doubt, verify and always ask for the full details of callers you don't recognize when they start asking questions about your organisation.*

d) ***Websites*** are a mine of information for any investigator. A WHOIS search can track down who owns the website, but you are able to register it to a PO Box and to use fake contact names.

Information on the website can be used to build up an initial impression on the nature and structure of the organisation. The main risk here is people using their real names and descriptions of roles. However, also consider how what you put on it may be used in civil injunctions where the level of acceptable evidence is much lower.

e) ***Keep files encrypted***. As a very simple precaution any sensitive files you have should be kept encrypted on your computer using PGP level encryption or disk encryption.

f) ***Need to know.*** In some cases this should be the guiding principal of how you work. Having meetings that define overall strategies or set campaign guidelines are a good idea, but when it comes to implementing the tactics to meet that strategy, working on a need to know basis is best, especially when there is a degree of covertness to be hand or your opponents are regularly involved in dirty tricks against you. As a rule of thumb, the more covert your actions and decisions need to be then the more you should be working on a need to know basis.

This is probably one of the more contentious points of security and can be hard to get right, especially in cultures which are quite open. Giving people a good understanding why not every fact should be public is the best way of dealing with this thorny problem in our experience. There is some evidence that both extremes, from complete openness to an entirely covert nature, can work for groups in the face of heavy state oppression; the difficulties come with mixing the two and is outside the scope of this booklet.

g) ***Information Management.*** This includes what is said in communications, but is extended to deal with other situations where information may be leaking out, especially if not everyone visiting your office is completely trustworthy.

g)a. Have polices in place to manage any sensitive information you may have; this should include where it is stored, who has access rights, rules on not leaving it lying around (in particularly if is letters from other people), etc.

g)b. Do you have backups in case it is all lost or stolen, with the backup stored off-site?

g)c. Do you have a system ready in case you need to get all sensitive information out of the office in a hurry?

h) ***Office security.*** When you move into a new space, secure it. Change all the locks if possible. Break-ins can and still occur with a variety of purposes. Likewise you need also to be aware of what sort of information casual visitor may also be able to obtain from your office:

h)a. To plant listening/video devices – so scan regularly and never say anything in an office you would not say to your opponents, including arranging meetings. If you have to make a sensitive phone call, do not do it from near your house/office either as these are just as likely to be bugged.

h)b. To examine your papers – never leave stuff lying around, especially sensitive material that casual visitors could see.

h)c. Obvious searches can be to create paranoia and fear in your group as well as to look for information; if you office has been visibly broken into keep this in mind. If your security measures are in place, then this should not be that effective from their point of view when it comes to gathering information. Part of their disruption techniques is to steal or break important equipment, so keep backups of material elsewhere and also physically securing your computer equipment with chains, etc. If possible set up an equipment replacement fund.

Ideally you will only let people you know well know where your office is and have access to it. If you must let relative strangers in, don't leave them by themselves. Keep sensitive material out of sight, and preferably encrypted on your computer. Things to watch out for in particular are

- Membership lists
- Info from confidential sources
- Campaign tactics.
- Personal stuff which point to your people's home addresses, etc
- Phone bills
- Minutes of meetings and up coming meetings written on wall calendars
- "To Do" lists

Locks we have been recommended as being generally the best are '5 lever multistead deadlocks'. As well as doors you should also lock windows, or put an iron bar across them so people cannot squeeze through. The state and professionals will have little problems with most locks so it is important to ensure that security does not simply stop at the door.

2.2 Advanced campaign security

If you are under active surveillance, there are many ways they can gather info about you. Below are some techniques to adopt:

a) ***Burn your rubbish***; it is environmental to recycle, but it is not safe. By rubbish we mean all paper work, envelopes, communications, printouts, etc and anything with handwriting or fingerprints on them – even old toner cartridges. Rubbish bins are a mine of information for the investigator.

When burning paper, do so until it is white and then scatter the ashes. One trick for burning stuff in most weather is to create a small furnace out of a tin can. Put eight holes about 1cm up from the bottom of the can, and use four nails in alternative holes. Rest the lid of the can on the nails and burn the paper in the can. To produce a faster, hotter burn, blow in the holes at the bottom.

Never trust this job to an outsider or temporary volunteers, and do it on a regular schedule.

b) ***Paper trails***; watch out for leaving paper trails when ordering your literature & merchandise. If your literature becomes a point of contention or you would rather it remained anonymous in relation to your campaign, work out techniques that either stop them locating your printer who can in turn point to you, or else keep your printers at arms length. That is, do not use your phones, personal mobiles or campaign addresses were possible. Collect in person and pay in cash (which may get you discounts as well). Destroy receipts as well where possible.

c) ***Sources*** are a vital resource to most campaign, and a very easy point to discredit you on if it can be shown that you let those details slip. Knowing who your sources are is valuable information your opponents would dearly like to have, so make sure it is kept very safe and minimise as much direct contact with the campaign as possible. Meetings should be secure (see below) and use dedicated mobiles for communication with them.

Be very careful of how you record them. Don't hold meetings in your office or at any of your usual haunts. Pick anonymous places away from your office and homes. Burn notes as soon as they are typed up (and encrypted), and stash dictaphone tapes elsewhere. When referring to sources use a codename and keep their real identities as secret as much as possible. Work on a need to know basis and discuss their existence as little as possible. Don't publish their work without their consent first.

Remember, companies you are targeting can be extremely paranoid about moles and infiltrators so you may need to give your source some security training so they do not implicate themselves.

d) ***Back-ups*** of your information and material are vital to keep your campaign alive. If you were to lose your membership list or research for whatever reason, accidental or maliciously, then it is potentially a crippling set back. Keep this sort of information backed up and your back up somewhere safe, such as the house of someone with out a direct connection with the campaign.

e) ***Tampering***; to detect signs of tampering, paint screws, locks etc with a UV pen, which leaves a mark invisible except under UV lights. If the markings are scratched then it indicates that they have been tampered with. These markings need to be checked periodically or there is no point doing this in the first place. Do it in a large cross, marking the surrounding material.

f) ***Autonomous structuring***. No one person needs to know everything and it is best that no one is put in this position anyway. The more a group can split into autonomous groupings working independently of each other the better. A network can consistently come together and break away into small groups and still be very effective. Perceived leaders will become the focus of attention and are more likely to be taken out.

g) ***New People.*** Volunteers, new campaigners and temporary staff are all potential threats. This does not mean that you should automatically mistrust everyone who comes in – that is just as detrimental. Use common sense and try them out before letting them know too much. With a bit of thought this can be done in a way that empowers them without making them feeling excluded. If they don't need to know sensitive details, then why tell them, or at least wait until they have proved themselves sufficiently to tell them. For example, do not give new people access to the membership list, keys or talk about inside sources.

When someone leaves, it is just as important to deal with the gap they leave behind. Delete computer accounts, tidy out desks and ensure that all responsibilities they held are covered or transferred. If in doubt renew security measures such as changing locks, etc.

h) ***Your communications*** may be tapped, and not just by the state. Don't say anything on the phone, or in emails, faxes or letters which could compromise you or anyone else. It is certainly not a good idea to discuss campaign tactics or name people as carrying out specific responsibilities, certainly not real names anyway.

Be prepared to purchase mobiles that are only for specific tasks such as sources and do not use them for other campaign purposes or ringing friends.

Tip: if they are going to bug your phone at the office or home, the chances are they will also tap the phone boxes close you your home. Finding remoter phones may be annoying, but it will also make life a lot more difficult for those monitoring you, but avoid favouring one.

2.3 Meetings (Open/Campaign meetings)

h)a). If you are having a meeting gather up any spare agendas left lying around at the end.

h)b). Depending on the venue and the political atmosphere, it may be worth booking them in the name of another group that sounds 'fluffier', and does not arouse as much suspicion.

h)c). Where contact lists are being passed around, etc, make sure they are not left lying around. The person initiating such a list has a responsibility for their fate. Such lists are a gold mine to investigators.

h)d). Not everyone making notes is a spy, but if it is out of place check to see if they are using shorthand, as a journalist would use. If there is a policy on this make sure it is announced clearly at the start.

h)e). Be friendly with the owners of a meeting place and have your stories ready in case they get too curious. If you are inconsistent they will get suspicious.

h)f). Finding out who is attending meetings is just as important as what is being said to those monitoring you, as it allows them to build up profiles on the people involved in the group. So if you do not want to be visibly associated with a group this is something to bear in mind.

2.4 Meetings (High Security – for planning actions, etc)

h)d. Don't use a pub, especially ones commonly frequented by other activists or which are likely to have the police/masons/your opponent's workers drinking in them.

h)e. Sometimes cafes and pubs are the only practical venues for a meeting.

If this is the situation, keep an eye on the actions of the other customers around you. If it is a meeting with a source, sit facing the door. Booths are not necessarily the best place if you cannot see those sitting around you, but it will depend on the venue.

Watch for out of place clothes or behaviour, eg not actually drinking the beer they've bought or not properly paying attention to what they appear to be focusing on. Amateurs are easily spotted, while professionals will not even look in your direction. If in doubt, move to see if you can cause a reaction.

Have a story ready in case someone does chance upon your meeting. Even if that person is an activist avoid referring to the person you were meeting as a 'good activist', or something else which would alert them that the reason the pair of you were together was anything other than innocuous. Having your lie ready means you do not slip up or your mouth does not run away. Turn the conversation away to something as soon as possible without being too obvious about it (look for related topics and not ones completely different). Avoid fidgeting and rushing off.

h)f. Vary the meeting places and times. Avoid doing the same place twice or otherwise creating pattern.

h)g. If you arrive at different times, do no hang around waiting to meet up outside before going in – it makes it obvious it you are having a meeting.

h)h. Avoid open spaces and parks in town centres. Ideally you want a place where other people sitting or moving in circles would look out of place.

h)i. The most secure way is to arrange a meeting is by word of mouth (never over the phone/text/email) to assemble at a point, and move on from there to somewhere secure, such as the middle of a forest. This gives an opportunity for any tails to be identified and lost.

Assembly points should not be railway stations, service stations or other places covered with CCTV which can be used to show that you gathered together.

Don't over complicate things as that leads to mistakes. Initial meeting points should either be known to the various parties or else easy to find.

h)j. If there are a number of you, have one of you go off and see how far your voices carry. This is particularly useful for when you are in a public venue such as a pub, where you might not have complete control over visibility.

h)k. If your group has regular meetings, arranging to meet immediately afterwards to discuss something more serious is not a good idea; it looks more obvious than you would think, and it is harder to shake off hangers on. Very private meetings should be kept separate, though the public meetings may be an opportunity to spread it by writing it on a piece of paper (to be burnt afterwards).

h)l. Turn off all phones and take the batteries out even before arriving at the meeting site. A cheap bug detector may pick up if there are any transmissions (i.e. phone calls) being made.

h)m. Punctuality is important; however if surveillance is spotted and the meeting is sensitive then do note attend even to warn the others as you may be letting those following you it is you are meeting.

h)n. Future meetings should be planned at this meeting if possible, and not left until later. Preferably do this by passing around the details on paper.

h)o. Even at very secure meeting points, one should still take care. Very sensitive stuff can be written down as opposed to spoken out loud. If you are using paper, first make sure you have a lighter to burn it when you are finished, but before you leave the meeting place.

Other materials you can use are etch-a-sketch pads for ease of destroying the writing if disturbed; or use rice paper which can be eaten much more easily than ordinary paper. If you are stuck with having to eat ordinary paper, do it piecemeal – putting too much at once in your mouth will give problems with swallowing it.

Directional and parabolic microphones are very powerful these days and are able to detect stuff even through some walls. However, there are limits to these tools and if you take sensible precautions, especially in the setting up of the meeting, then these should be very low on your scale of fears (unless you are under some seriously heavy surveillance). If they are a concern, then rooms with out windows are good, or cover windows with heavy drapes to muffle sounds. Add further problems by putting a stereo speakers next to the window.

h)p. When setting up meetings, depending on the degree of covertness and geographical distance of the people attending then consider using PGP, face to face contacts or coded postcards/birthday cards for exchanging the initial meeting place / dates.

h)q. Take care you don't give away a meeting place by scouting it out too much (the same goes for sites of actions).

h)r. Consider having reserve meeting places if there are unforeseen circumstances such as travel delays or the original meeting place is compromised in some form (police, overcrowding, etc).

If one of the parties is delayed, this allows the other parties to leave, turn on their phones to get a statement of how long they will be (perhaps in code) that a delay has occurred, and then for the parties to move to the next destination. Note: if there is a large time delay it is best not to go to the meeting point until the appointed time so as to avoid hanging around and attracting attention. Finding the place and going somewhere else to wait is normally okay.

2.5 Secure information transfer

Meetings, telephones, letters and emails are not the only ways to transfer information. There are a whole other battery of techniques available for use, many including drops where information can be exchanged without parties meeting each other, etc. However, these are more useful for situation where knowledge of contact is the most important things to be avoided, or all that is being exchanged is sensitive information. For most activist groups these will not be significant issues, so we will not cover them further here. Many are also no longer particularly available in modern Europe or as secure as they once were. Others require an extensive infrastructure and/or hierarchical network with penetration into the infrastructure of the country itself, so again are not particularly suitable for the European or US activist.

However, where communication to set up meeting is difficult to achieve securely (eg lack of PGP or geographical distances) then a meeting can be set up by exchanging postcards, letters, etc where there is something in the contents which indicate the actual meeting. For example, a fake letter where the senders address is for example17 Green Street, London, W18 4QR, which could translate as 17.00 hours on 18th April and Green is code for the venue. This has to be done right if some of the recipients of the letters are having their mail watched - do it too often and it could be picked up on as being a communication technique – however, to offset this:

- Vary methods of sending (letters/postcards/etc). Letters are better than post cards. Birthday cards, etc are also good to use as well as being far more difficult at stopping casual investigation.
- Use the names of previous occupants of the house the post is being sent to, or a fake individual.
- If the meeting involves more than one person in an area, rotate the letters around the people (though that has security issues in itself).
- Use friend's workplaces, especially if part of a big company.

Maildrop boxes using free email mail accounts can also be used to set up meetings and exchange information. Remember to use codes for names and not to send the emails – simply store the messages in the draft's folder. Points to remember are to

- Delete messages once they've outlived their usefulness.
- Access only from internet cafes.
- Never send passwords over the Internet when bringing other people into the loop.
- Never mention personal names of those using the drop.

More sophisticated systems can be built up as well, with replies being put into separate maildrops. For example, Person A leaves a message in Mailbox Z. Person B reads the message in Mailbox Z and sends a reply which they leave in Mailbox Y. Person A reads the reply in Mailbox Y and returns to Mailbox Z to respond in turn. And so on. It is not hard to make this more complicated and secure, but remember to balance out with risk and effort and that it does not become an impossible system to use.

There are pros and cons to using common freemail ones such as Hotmail, Yahoo as opposed to RiseUp.net, Resist.ca, etc. The former have the advantage of being anonymous by being buried among the vast numbers of other users but poorer security; the latter have better internal security but draw attention by being so associated with activism. Our opinion is that either approach works and are equally valid.

Along similar lines you can consider physical maildrops (not good for those under surveillance) and personal ads in newspapers.

2.6 Gossiping

This is something very hard not to do, especially when internal divisions arise in a group but small splits are something that can be used by infiltrators and others listening in to sow dissent, or even turn people into grasses. It also helps break down trust within a group so affecting its strength and campaigning ability. It is better to have a professional attitude, and it things get very bad to call in mediators.

At the end of the day, productivity and motivation are more important than being part of a group of friends. An affinity group does not necessarily need to get on as friends, as long as there is the sense of trust that everyone is going to follow through with their work and support if necessary.

2.7 Being monitored

We discuss listening and tracking devices under personal security. However, it does not mean that this is all they will use. Depending on your situation, if your office is suddenly the focus for an action or the building you are in has a flux of activists through it the chances are it will be monitored and not discretely either. Watch for the following:

I. People taking photographs of the building
II. People taking down licence plates in the vicinity
III. New people attending your meetings and showing excessive interest in other members or simply not fitting in.
IV. Keep an ear out for changes in attitude from landlords, other people in your building, etc – it may suggest that they have been approached and lies told about you.
V. People sitting in cars for prolonged periods at your office or home.
VI. You see the same faces repeatedly around your homes and offices.
VII. Increases in police patrols passing by.
VIII. An increase in numbers of people being approached to be a grass.

Watch out for delays and tampering with your mail – for example

I. Regular tears in parcels.
II. Corners of envelops broken.
III. The mail arriving late and all at once.
IV. Mail regularly disappearing.

Remember, many of these warning signs by themselves are not sufficient to indicate that you are being monitored, but if they all start happening and you are running a campaign threatening to be successful then the chances are you are being watched in someway.

Something you can do is put in formal complaints to Royal Mail, etc about the problems. You can even complain loudly over the phone for those interfering with your post and phone to monitor you more subtly – it has worked!

Those opposing you may also be interested in killing off your campaign. In some cases it has been known for them to break in to an office to search for information and to damage important resources. However, these days it is more likely that the police will raid the office under spurious reasons simply to seize equipment you need to function. Backing-up of anything valuable is important!

3. Dealing with infiltrators and grasses.

This is not a pleasant task, and fortunately they are few and far between. Infiltrators are expensive for the police to run and more likely to be favoured by corporations with deeper pockets. Grasses are preferred by the state as they are cheaper than employing someone full time and without the attendant risks. You may also have problems with journalists trying to get information for a juicy expose on you. However, in our experience these can be quite easy to spot by the pointed nature of their questions, their superficial knowledge of issue and their inappropriate dress sense.

Note, infiltrators do not focus solely on militant groups, or those successful in disrupting the status quo; attention is also paid to groups which may command a large amount of favourable public opinion, which in itself is a threat to the state – for example the ploughshare/peace and anti-apartheid movements.

However, to call someone a snitch is a very serious charge to put at anyone's door, and you need to be ready for the personal consequences of backlash against yourself, and possibly split the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone's back as that is how nasty rumours start as misunderstanding develop. Even passing accusations without real factual backup or research are to be avoided.

3.1 New people

The first thing to do is to make sure before commenting on whether someone is dodgy or not. Many people when they first get involved are often excited by what they have read and heard. They may not have had a chance to adjust to our security culture and needs. It does not make them spies, and jumping down their throats immediately or not explaining the situation to them because you've gone into paranoid mode will do nobody any use and simply do long term damage as they get driven out or put of. What may seem obvious to us is only so because of our experience as activists; it may not be that way to an outsider so allow them that initial space. Explain to them first! We were all young, naïve and eager to take action once, so think back to what it was like then.

If they still do not get it, then is the time to become somewhat more concerned. If your campaign is structured securely, a grass or infiltrator should only be able to achieve limited damage, plus you should not be exposing new people to sensitive material anyway.

It is always good to visit people at their homes or just learn about their backgrounds. Maybe even meet their parents if such an opportunity arises. This helps build the trust. But the main thing is to avoid letting paranoia taking over – think back to when you were first joining your group or movement and all the mistakes you made then. People do not join a group fully clued-up, so don't expect them to be. A group run along paranoia lines to the point it near impossible or exceptionally impossible to join is not going to go far. This sort of paranoia also prevents accurate instincts from developing.

Saying that if they truly believed, new people would put up with the paranoia and exclusion is a poor excuse, and symptomatic of a group which is not dealing with security on a rational level.

3.2 Do you have an infiltrator?

Why would you suspect you have an infiltrator in the first place?

- Things going wrong when they've not been doing so previously.
- Your opponents seeming to know what you are planning (though this may be part of a disinformation program to cause infighting).
- Constant internal disruption.
- You are a high profile campaign.
- Your opponents have a history of covert action against campaign groups.

There are ways and means to identify people you suspect, but we suggest you approach an organisation that with experience in dealing with these issues. In our experience though, many infiltrators give themselves away by being too obvious.

Infiltrators tend to go for positions were they can either do the most damage or get the most information. Watch out for people who:

i) Volunteer for tasks providing access to important meetings and papers such as financial records, membership lists, minutes and confidential files, even indirectly such as typing up notes and 'recycling' the paperwork. Often they are not the most glamorous but quite dull tasks so people are happy to pass them on to others despite how much they expose the details of the group's members.

j) Do not follow through or complete tasks, or else does them poorly despite an obvious ability to do good work.

k) Cause problems for a group such as committing it to activities or expenses without following proper channels; encourage the group to plan activities that divide group unity.

l) Seem be in the middle of personal or political differences that are disruptive to the group.

m) Seek the public spotlight, in the name of your group, and then make comments or present an image different from the rest of the group.

n) Urge the use of violence or breaking the law, and provide information and resources to enable such ventures. This depends closely on the nature & atmosphere of your group. Context is important here, especially on how heavily monitored the group is.

o) Have no obvious source of income over a period of time, or have more money available than their job should pay.

p) Charge other people with being agents, (a process called snitch-jackets), thereby diverting attention from him or herself, and draining the group's energy from other work.

q) Are inconsistent about their background – lies at this level are hard to maintain completely, and slip-ups do occur; take note of inconsistencies and follow up on any 'facts' about themselves that they tell you.

r) Will be regularly overgenerous with their money buying people drink and/or drugs so getting activists into a condition where they are more likely to be off-guard and talkative.

s) Make false claims and exaggerate about their background in other movements.

(This list has been adapted in part from http://www.publiceye.org/liberty/whatbugs.html - it is also a useful article for U.S. readers wishing to know where they stand legally with respect to infiltrators and spying.)

Remember, none of the above are by themselves proof that you have an infiltrator. It may be that information is leaking through carelessness or bugs. Or that you simply have pain-in-the-arse in your group who needs to be dealt with (we will not deal with this here, but it is a security issue in some ways as it causes others to become disaffected, feel betrayed, etc). See a professional mediation group, but do not let it continue unchallenged to the point it starts affecting the group's work.

3.3 Initial Action & Gathering Evidence

Once you are sure your suspicions have substance you need to start gathering the evidence to back them up before moving to deal with it. Don't move before you have the evidence as you could simply end up causing an environment of mistrust in the group, leading to ineffectiveness and splits. To gather evidence consider the following:

I. Contact someone experienced for advice, or a group such as the Buro Jansen & Jansen (www.burojansen.nl) who specialise in this. This is as much for legal as practical advice.

II. Put processes in place to protect sensitive material or planned actions; often if you close off the information supply your suspects have been accessing they may soon drop out anyway.

III. Put together a file of all question marks over the individual with as much evidence where possible. This should include accounts of suspicious events/statements. You need to record dates, time, places, people present, and other material that puts the event into context. Also keep a note of any disruption to events or unexpected presence of police that may be associated. Keep this encrypted as it is valuable material to your opponent and you do not want your suspicions to break our prematurely.

IV. Discretely ask the suspect about their background and personal life and check it out. It is very hard to lie consistently all the time, especially if you are probing in areas where they do not have a cover prepared. Remember, cover stories tend to be a mix of both truth and lies. Make notes of any inconsistencies but allow for the fact that people often exaggerate anyway just to fit in.

If they claim to be involved in other group, approach that group and maybe with a photo in case the suspect has changed their name. Often when an infiltrator has been exposed in one group, they simply move onto other ones in related movements, using their experience and contacts to make the transition easier. However, watch out for other groups tipping off your suspect, so be careful if you are approaching third parties for help and ask them to keep quiet on the matter.

Some ways to actively check out their claims is by ringing their 'work', or following them. A hint something is amiss is where a person who drives an old car to meetings, but can be found driving something much newer at home.

Another thing of use is to distract the person and to go through their possessions to see if there is anything incriminating – particularly useful at gatherings or meetings where there is limited time to evaluate someone who clearly sticks out.

V. As you progress in confirming your suspicions approach others you trust implicitly to help you build you your body of evidence. But do it carefully, as it is hard to prevent people's suspicions from leaking into meetings and social events. However, if several people suspect a person independently then that is a good sign you are on the right track – as long as it is not just on the ground that the suspect is a new and keen person.

VI. Set a trap. "Arrange" an action or meeting that the suspect is informed of and check to see if there are any police or extra security waiting. If the subject is talking about their involvement with others in the group this may be tricky to organise. It needs to be planned carefully, and may need to be done more than once to catch the person out, especially if they are in for the long terms as they will wish to avoid raising suspicion before they have had a chance to properly integrate with the group. Also one set of unexplained extra presence can be explained away as bad luck; more than once ceases to be coincidence (though it may be bad security practise on the behalf of the suspect such as talking openly over the phone about it – in which case you know you've a liability anyway).

Avoid acting too out of character so as not to tip them off that it is a trap, or doing it in a way which may arouse suspicions from other interested parties that there may be something worth investigating.

Often, in such a set up the suspect, if they are dodgy will back out rather than do something incriminating. Either way you know they are not up for it and not to be given trust likely.

VII. If you suspect you have an agent provocateur consider getting them to incriminate themselves - have a dictaphone ready so when the opportunity arises you have the evidence in case anything is used against you in the future, that it was the infiltrator or the grass who tried to entrap you. Keep the recordings secure (not in your house) and make backup copies. Consider talking to a lawyer you can trust.

Most police infiltrators will try to avoid being active in anything that may be construed as illegal as this will compromise their evidence in court – especially if it can be argued they instigated it or had a chance to prevent it. Private investigators may be less shy.

This is an extreme action and we really cannot recommend that you carry a dictaphone around as it put other activists who are genuine at risk. Plus if people notice you might be the one who ends up getting suspected. Only do this if you have a very strong belief that someone is attempting to set you up.

VIII. There are other problem types besides infiltrators. Some from the media will deliberately put forward mad ideas in order to create a more exciting response or story, so setting up opportunities for their stories. There are also those people who are genuine control freaks and will disrupt if they cannot get their way within a group, and end up destroying it out of petulance rather than deliberate mischief.

What is important is that you do not go public on insufficient evidence – what happens if you get it wrong! You could loose a person who could subsequently be turned against you, and you can end up creating a bad atmosphere in your group, disrupting your effectiveness. People can turn on you as well.

3.4 Exposing the infiltrator

When you have gathered what you feel is sufficient evidence, you need to act on it. How you do this depends on the horizontal/vertical nature of your group. For non-hierarchical, grassroots groups, the best approach is to get the information out to the group, which you need to plan for.

Firstly, arrange a meeting between a few of you with the suspect and put your evidence before them. Watch their reactions and carefully note their explanations of the evidence. Normally, by this stage the evidence should be sufficient for them to chuck it in – though maybe not without shouting that it's all a hoax but they cannot work under these conditions, etc. If you are going to expose someone subsequently, get a photograph of your infiltrator while you can.

Next, arrange a full meeting of your group, and put the case before them. It is wise not to announce the true purpose of the meeting beforehand, as if others talk to your suspect they may tip them off inadvertently. You do not want to announce your allegations without having the meeting first. Ideally you will challenge the suspect shortly before the meeting. If they do come to

the meeting to defend themselves, they will be better prepared and change their story to adapt to the evidence, so you will have to challenge them on this – this is the main reason for having witnesses at the initial confrontation.

At the end of the meeting, ask the suspect to leave the room so the rest of the group can come to a consensus on which side they believe. It may be worth you leaving as well to avoid claims of bias. If they agree with you, then ask the infiltrator to leave the group

If your suspicions cannot be confirmed more than circumspectly you need to tread more carefully. A potential approach is to confront the person with your suspicions as it may be enough for them to back off, but be prepared for the situation to backfire and they deny anything (after all they may be innocent). Continue to monitor them.

If you have approached someone accusing them of being an infiltrator, and they have left the group before you have had a chance to speak to the rest of the group you need to act fast, and get a meeting together. Failing this, you need to contact them as soon as possible with an account of what has happened and be prepared for the following:

I. Primarily you need to provide your group with the information to back your claims up. It is important that things are clear and transparent to ensure that you are not seen as abusing power.

II. The exposed infiltrator may be angry and attempt to turn the tables on the people who have exposed them by causing disruption in the group, for example by ringing other group members and telling them lies about their exposure.

III. You may have to explain to some group members why they have not been trusted with this information to date, as they may be hurt by the perceived lack of confidence in them

For hierarchical groups, speak to key people you feel can be trusted with the information and ask them on how to proceed.

3.5 Dealing with the fallout

Once the infiltrator has been exposed consider doing some of the following to protect your reputation and to repair the damage to your group:

s)a). Consider going to the press to highlight the issue, though this clearly depends on the nature of your group as to how appropriate it is. It is a tactic more suitable to more mainstream groups.

s)b). Let other groups know through established channels. Publish a photograph of the person on relevant websites and other news services (magazines, Indymedia, etc) so others are able to identify the as infiltrators, so that they do not fall victim to the same individual. Be prepared to substantiate your accusations. Send a letter to all the groups you are connected with an explanation and what you are planning to do to minimize the problem. An example of how one infiltrator was exposed and advertised is the first “Notes from the Borderland” by Larry O'Hara, which deals with the activities of the infiltrator Tim Hepple/Mathews.

Expect some uninformed backlash and loss of reputation, but it is better this happens than people find out through rumour which will affect your credibility much more. The danger you face here are rumours spreading unchecked.

s)c). Put in processes for preventing it in the future – can help retain your reputation, following any backlash over the exposure of the infiltrator.

s)d). Put in to place processes to minimise the damage to your group. This is important to stop unnecessary paranoia and infighting that can arise – especially where some members do not fully believe the evidence gathering or there have been sexual relations between the infiltrator and group members. Some group members may not want to accept that they have been conned in this fashion and their objections may be based on this.

s)e). Change locks, passwords, etc. and analyse the affect on materials and campaigns they may have been involved with.

3.6 Gatherings

These pose a different set of problems. However, final authority normally rests with the organisers, or a sub-committee specifically set up to deal with this issue, to ask the suspects to leave. You do not have much time to gather evidence, but in our experience spotting them is not particularly difficult as infiltrators do not go to significant amounts of effort to cover themselves at temporary gatherings.

Ideally a couple of people will get together and agree on a strategy for dealing with the person, including approaching them with questions (either confrontationally or subtly as the occasion requires). Some of these people should be recognisable individuals

to give the group doing this some legal standing in the eyes of the rest of the gathering, or else it should be convened and authorized by a spokes-council where appropriate. The last thing you actually want is a debate on the process when you are actually trying to have an infiltrator leave, or a self-appointed mob trying to deal with the situation.

Ask the following questions about the suspect person:

- When they take notes at what point do they do it?
- Who are they watching and listening to? How keen are they on particular individuals and at writing down people's names?
- How are they making approaches to people?
- What sort of questions are they asking of people; are they showing repeated interest in illegal or violent activity, or being exceptionally nosy about people?
- Are they asking questions about 'leaders' or that simply do not sound right (eg. "Where is your central communications unit?")
- What about their clothes, watches and shoes (eg leather at an animal rights event)?
- How did they arrive, and who with? Have they walked and left an expensive car out of sight?
- Who do they appear to know, if at all?
- How clued in are they to the issues?
- Do they appear to be drinking but actually are nursing the same beer through the night?
- Are they taking notes in shorthand?
- Have they professional journalist equipment with them such as dictaphones and cameras?
- How have they learned of the event, and what are their reasons for attending. Who do they claim to be in contact with?
- When you go through their bags and tents, do you find anything suspicious

Generally infiltrators at such events come singly or in pairs and do not know anyone else there. They can latch onto a group of people and act as if they are part of the same group, something that is easy to check out so simply because they are hanging out with others does not necessarily mean that they are their friends. They may even be from other countries.

What often happens in these situations is various people start to get suspicious of an individual and start pointing them out to the various organisers, etc. This is why it is worth having at least one or two people working on this who can take the various feedback and then make the appropriate call to investigate further. Likewise, if someone is being unnecessarily paranoid then their fears can easily be laid to rest by locating the suspect's friends, if they exist and check

In a number of cases, a suspected individual has been able to provide *bona fide* credentials on questioning and being able to be identified as a friend of a particular group once challenged, so do not march individuals straight out of the venue.

Once identified to people's satisfaction, march them out of the venue. Use reasonable force to eject them but do not get excessive. Most will leave of their own accord having been spotted, but some will kick up a fuss (journalists are quite bad for this) thinking to raise support for themselves that will cause people to back off. If there are people at the gate/entrance then they should be allowed to see the person to avoid letting them back in later on. Taking photos of the individual is good for later identification.

3.7 Grasses after arrest

This is particularly unpleasant but sometimes activists do crack or turn due to police pressure / persuasion. It is not always used directly against you but there are signs you can watch out for. However, don't listen to police telling you that your mates have turned on you, as that is a standard tactic they use to break your resistance and is generally a lie.

In the UK when people start 'grassing' or 'singing' in a post-arrest situation they are separated from the other defendants, and 'public immunity certificates' are issued to prevent the fact that they are talking being made public. Often their evidence will not be used directly, so it may not come immediately apparent. Your solicitor should be able to let you know if this has happened, albeit only indirectly. Public immunity certificates may also be granted in favour of witnesses you may wish to call to support your case. As a rule of thumb you should be very hesitant to trust anyone who has a public immunity certificate issued for them.

Where the grass is up on charges by themselves, they may get ridiculously low sentences and the police suddenly know where to target people effectively or start quote very specific evidence in interviews.

Other evidence that someone has turned is the quality of treatment they get when arrested. For example, one turncoat received a TV in her police cell when she was picked up while hunt sabbing.

It should be made very clear that anyone who gives a statement against other activists will be made very unwelcome by the rest of the movement. They should be named and shamed along with having their photos published in relevant forums. However, if they are part of a larger trial, this should not be done until after the end of the trial to protect other defendants (it is their call as they are the ones who will suffer the worst).

Other 'infiltration' methods

If someone approaches you as media, try to check their credentials – ask for their cards, and phone the switchboard of the newspaper/TV/radio station they claim to work for to check they are genuine. Mobile numbers are not good enough. In more sophisticated set-ups the phone number will also be genuine so check their presence online or in the phone-book to gain confirm their identity and that the numbers are indeed going to genuine offices.

If it is someone wanting to make a film about your 'cause' or campaign, check out the production company they work for and ask to see previous work by them. Film & TV production companies are a good front to approach activists with and attempt to get close to them, especially with their requests for visits to offices and to meet other activists – deny these whenever possible. Never believe the "put your side of the story" line. Carefully manage what they are allowed access to and when they can record.

Other agencies can be front organisations set up to get your trust, so just because you are dealing with someone from another organisation with supposedly the same aims as yourself, unless they have a proven track record then treat them carefully when passing on details about yourself, etc. Even if they are a proven group, they may have an unspotted infiltrator or slack security, so pass-on personal or sensitive material with care.

Sometimes the media approach may be genuine, but media are always looking for the exclusive footage and 'inside scoop' so have a completely different agenda to the activist/campaigner. They will not hesitate to set up activists, so you should always be on your guard around them, and be very careful about how much information you provide them – they can end up doing the state's work indirectly for them.

Given the prevalence of video-camera's these days there is little reason for media to come on covert actions at all.

4. Security for Actions

Actions come in many different forms, each one with its own security needs. Many ideas mentioned under campaigns and personal security may also apply here so we will not duplicate them here.

In this chapter we mean by actions a wide variety of events and deeds. Not all tips will be applicable to every situation, but we hope that what is and what is not is obvious.

4.1 Choosing people

Depending on the nature of your action you may need to be careful about who you inform regarding it.

4.1.1 Approaching people

Approaching potential participants in an action needs to be done correctly. Ask people what they feel about the type of action you are planning in general, on an abstract level to check that they would be interested in what you have to say. As affinity groups are built on trust (and often friendship) you will know for the most part how individuals file or whether they are "up for it" in general.

If you ask them about doing an action and they initially say no ask about it later, unless they are expressing an interest in being involved, then tell them it has been called off. Once committed warn people against backing out later or talking about it. The degree of secrecy needs to be made clear right from the start so people are clued in otherwise there are inadvertent breaches of security made early on. As someone putting together an action you should NEVER assume everyone automatically has a clear idea of the level of security needed – it is up to you to remind them.

4.1.2 Gradually introduce people

It is best not to throw people in at the deep end, unless you are very confident in your action and in them. Better it is to work them up the ladder, watching how they react in different situations, how well they keep their cool, etc. Sometimes people make out to be more confident and skilled than they actually are. The problems will not become apparent until they are actually in action, by which point it may be too late.

If you are not 'invited' to actions and feel bitter about it, put yourself in their place and understand that their security needs may be playing a part. Those involved need to be wary about not letting it slip so inviting inopportune questions – this includes behaviour as well as what is said. Do not arrange or hint at meetings in front of those not involved as it is quite disheartening to future activists.

4.1.3 Watch out for bravado

People will talk themselves up, and make out to be more experienced than they really are. Recognise this in people and be ready for it in case they end up bottling it and leave the rest of you in the lurch. Often they will not even turn up for very low risk stuff or get very uptight and show erratic behaviour when they do attend. It may be better to be blunt with them by saying that you haven't worked with them enough yet, and that you personally don't feel comfortable in that situation, especially one where there is a lot of risk. If they are genuinely committed to movement happening they will accept this.

If you suspect that someone is more boasting then action, then check out if they've actually done the stuff they've claimed (eg, fly-posting, graffiti, etc.)

4.1.4 Watch out for the boasters

Like with bravado, these people can be a risk. It is hard for them to not tell people about what they are up to before and after an action, even after they have been warned to secrecy – some become smug and extra secretive, which can be little better than giving away that they have something to hide. So when introducing people into your affinity group note their ability to keep secrets as they become involved more deeply. At the end of the day our main reason for being active is to achieve social change or save lives, not to make people feel better.

4.1.5 High profile people

Some people are naturally under a lot of attention, whether by police or otherwise. This maybe due to their apparent organisational role or simply their history of being arrested (especially for serious offences). Even though they maybe excellent activists, they may end up compromising your action by bringing unnecessary attention to you. If they don't need to be involved, keep them out of it.

4.1.6 People with issues

Although we like to be inclusive and bring many people into our movements, it does not mean everyone is suitable for every action you plan. If you are going to take risks then you have to be doing it with people you can rely on if things do go wrong, or can be counted on to do their part to make sure that things do not go wrong in the first place. We are active not to run self-help

groups, but to make changes. That may sound harsh, but so is loosing your freedom because of someone else's personal issues which they were unable to put to one side.

Drug users and heavy drinkers are a liability, as are people with money-draining habits such as gambling. As well as being unreliable, they are much easier to turn or trick into talking. Recently, much of the "Green Scare" in the US, where large numbers of ELF activists were arrested up to a decade after they were involved, was by using one activist's heroin addiction to break him and use him to leapfrog into the rest of the groups and to entrap people by talking about what they had done years previously.

Addictions can also cause people to fail to carry out important tasks properly and lie to cover up their mistakes, so putting the action or rest of the group in jeopardy, this runs the gamut from not turning up on time to go to a hunt sab or demo to acquiring equipment and being in place at the right time on a covert action. Another problem is when people get argumentative at unsuitable times such as on the way to an action, jeopardising the morale and energy of the group, and whether the action itself goes ahead. This can apply to people with addictions or mental health issues.

We would also recommend against bringing along people with mental health issues where the stress of taking risks may prove too much, or that later on, after the action, they may not fully understand the need for maintaining security in respect to it.

If you are a heavy drinker, drug user, etc consider how you may be jeopardizing others so consider moderating your consumption so you are not losing control, or else stop doing actions where you would have knowledge that could put others at risk.

A less obvious risk are people who have personal reasons for joining a group and are not necessarily motivated entirely by the aims of the movement. They may consider activists as cool people to hang around or as introducing an element of excitement as they swing close to the "danger". Others are simply needy people who are preying on the inherent kindnesses to be found in the people active in social movements. It maybe that, depending on the needs of your group and actions, that such nicety needs to be put aside. People with the wrong motivations are less likely to understand the need for security and often talk without thinking, even to police, as they like the attention. It is not malicious, but just how they are.

4.1.7 Security and your affinity group

The final point when bringing your team or affinity group together is to ensure that everyone is working to the same standards. Differing standards may mean that some people are not doing enough to keep the group secure and others are being too paranoid to the point it is disruptive or disempowering. Discuss it through and make sure that everyone knows what security measures they have to take and why. As in campaign security, it is best to reach a consensus whereby everyone is clued in to the needs of the situation and acts appropriately. Such discussions are also a good way to spot people who are only giving lip-sync to the requests or being too blasé about security.

Security measures reached by consensus and understanding are much more likely to be adhered to than ones imposed on people. Also, it makes it easier for people to be pulled up if their security is getting slack. A classic case of this is mobile phones at gatherings. If the group decision is that mobiles phones have batteries removed and not taken to meetings, and that decision is clearly broadcast, then it is much easier to call people up for 'lapses' where they are turned on or brought to meetings.

Have a security run-though before the action. Make it clear that these are not a case of someone being on a power trip or distrusting people but good security practise – mention it at the start of planning so people know to expect it. Even experienced people make mistake and it shouldn't be a case that individuals are made to feel embarrassed by slip-ups. A security run-through is there to refresh and remind people, ego aside.

Create a situation whereby people can feel able to admit to mistakes. It is better to have it out, than hidden where it may come back to haunt you. Likewise, if you have made a mistake, it is important that you own up to it, even if it jeopardises everything, so your group doesn't go through with an action which may have been compromised. You have a responsibility to the group you are working with. Also, if it becomes clear that you were the one responsible for the security breach and didn't let people know then people will not trust you enough to involve you in future actions.

When setting up an action people do not necessarily have to be practising security at your level, but it may be an opportunity to teach them about it through example, explaining why you are taking certain measures.

4.2 Scouting out the area

When checking an area out do not look out of place. Dress appropriately, smart if necessary or a Barbour jacket and boots in the country, and depending on the area have a cover story ready. Basically the more natural you act the better – and don't be rude to people you encounter.

Plan any surveillance carefully, and pay attention to the times you will be going in and out of the area. If doing walk/drive-bys do not do it so much that your face becomes recognisable, so if the police show someone a photo of you they would be able to

identify you. Don't forget to use counter-surveillance techniques to ensure you are not being watched yourself so compromising the action and its participants.

Before you leave decide as many of the factors you need to know about so you gather as much information possible in one go. This saves repeat trips back to the sites to fill in gaps. It is always worth doing a brainstorm on this with other key members of the group who will be involved.

For relatively low-key actions where there is little chance of you being arrested, there is no reason why you cannot think up a blag story to get entrance to the site, or even just pretend to be lost. It doesn't compromise your security that much, if at all.

For covert actions, check out what else is in the area and let the rest of the group taking part know as well. For example, you don't want to run in the direction of a farm where dogs who will raise the alarm. Similarly if there are likely to be any "curtain-twitchers" or other nosy neighbours that could be a problem. Know your access points in and out and make sure your drivers are familiar with them. Identify and scout back-up rendezvous points should you be forced to scatter.

Some useful techniques are to:

a. Go in male-female pairs so you can act as a courting couple if necessary.
b. Bring a dog lead and pretend your dog has run off and you are looking for them.
c. Chose an appropriate looking vehicle to blend in better.
d. If staking out, avoid smoking, and don't drink lots of water/coffee or you will end up having to make regular trips to the toilet.

4.3 Planning

Planning is good. It gets you in the right state of mind. Decision-making is much quicker and when the unexpected happens, you are better able to handle it. No plan is perfect, and you should be prepared for things to go wrong. Hence have backup plans for when things do go pear-shaped, such as alternative meeting points, and when just to cut your losses and leave.

Rehearse your plan with everyone together (or who needs to be together) beforehand. It is a good idea for people to know what to expect of others and helps build up the strength of the affinity group. If part of your action is going to require people to leap fences, make sure they are going to be able to do that – little things like this are often assumed as other people make them look easy, but the reality is sometimes otherwise.

Make people fully aware of the risks and that they are prepared for the consequences. Recriminations afterwards are destructive as well as being too late. Be ready to answer pointed questions as people will be concerned about the risks. It doesn't mean that they are infiltrators, but keep things on a need-to-know basis, as much as is reasonable.

If there are several parts to an action, not everyone needs to know who is doing what. This means if one of the groups is compromised it doesn't necessarily affect the others sets of people. This 'need to know' basis for actions has been one of the most successful features adopted in actions and proven to keep people safe.

In the run up to an action and afterwards don't start acting strangely, extra paranoid or suddenly changing your habits. The chances are that these will bring more attention to you. Act as naturally as possible, as if there was nothing about to happen, or has happened. Discretion is much better than being paranoid. Have cover stories and alibis ready for your actions and whereabouts.

Tip 1: Often actions may involve known activists from elsewhere. Don't suddenly have an influx of visitors coming to your house which may indicate that there is something going on worth investigating.

Tip 2: If people are travelling to the area by public transport to be picked up, don't pick the nearest stop or station to your house or to the place of the action; where possible do the one before at least, so there is a bit of distance between them.

Tip 3: Don't create changes in your phone call patterns in the run up to or immediately after an action to particular individuals. That is, do not ring someone more often or less often than usual. The fewer connections that can be directly drawn between individual parties the better.

4.4 Communications

Most of what was said in the section on campaigns regarding meeting to discuss and plan equally applies here. The nature of the action depends on how open you can be about it. If you do it over the phone/unencrypted email/text messages the chances are the police or your target will become aware of it. This may not actually matter, and if it doesn't then don't worry about it. The only thing of concern in this situation is that they may be able to single out one or two people as doing all the organising and focus their efforts on them, so it is not appropriate if you are planning to keep a low profile.

Basically, do not say anything on the phone or by email that you would not be prepared to stand up in court and say to a judge, or that will tip the authorities to the fact that you are planning something. Code words shouldn't be obvious, and avoid using obscure, half-broken sentences. Phrases such as "are you coming to that funeral/party" are too commonly used to be effective any more. The best approach is to arrange to meet people and pass the message on either verbally, or by writing it on a piece of paper. Tip: always carry a lighter so you can burn the paper immediately you are finished with it. It is easy to forget to burn it later so you end up carrying it around in your pocket.

Setting up a meeting is ideally done face-to-face. It is bad practice to simply turn up and have a meeting there and then. The less that can be said at the initial invitation the better. If someone is doing the organising, they should meet with people individually and test their commitment to the action before letting them in on who else is involved. Avoid organising a meeting around your social group or at a social event as it will rapidly become obvious to others not involved that something is up. This is not always possible to avoid but you need to be aware of this problem.

If visiting someone, you can have a completely irrelevant conversation with them while passing them a note about what you actually want to talk about.

Never have at meetings people who are not going to be involved, no matter how good an activist or friend they are, or even if they are otherwise part of your group. For starters, it makes them an accessory. A classic infiltration by the state of the far right was a man who used to sit in the pub with the gang until he got so familiar to them they discussed their plans in front of him.

Tip: sometimes discussion comes up during the action; be ready to deal with it, especially as important points may need to be clarified. To help with this, have an *etch-a-sketch* board from a children's toy store in the car; it looks innocuous so helps detract from any impressions you may be up to no good, and it is also a good way of passing messages to each other that can be easily erased in one quick go.

4.5 Acquiring Equipment

Buy materials and hire vehicles well out of your area. Be prepared to have to put time and money into this. Avoid using your own vehicle if there is that option. If you have hired a vehicle, do not park it near your house. Where possible avoid using credit cards, though it is often hard to hire vehicles without one.

Phones should also be purchased out of your area. Get pay-as-you-go models and when using top-up cards pay in cash. When purchasing them, you are generally asked for details to give for insurance or warranty purposes – have false ones ready to give to them. If possible buy from second-hand shops without CCTV.

Burn packaging, receipts and other such materials that may link you to the equipment and which are not necessary to keep. If there are serial numbers, etc, consider filing them off or otherwise removing, as if the equipment is discovered this can be potentially traced back to the shop where the piece of equipment was purchased and hence maybe to CCTV implicating you in their purchase.

Wear a baseball cap and non-distinctive clothes when making purchases; consider buying a set of clothes from a charity shop and once all your purchases are made dispose of them. It is best to dress down and blend in – wearing radical T-Shirts is definitely not a good idea. The longer the gap between purchase and the action the better as the less likely shopkeepers are going to remember your face or have kept the CCTV footage when the police come snooping. Also with this, if you are unfortunate to be under surveillance, they will be more ready for you to do an action in the next few days after you've made your purchases; which may go away after a while if they see no activity to accompany it.

When bringing material back for storage, especially if it is in someone's house, wrapped it up so it cannot be identified. Consider putting newspapers and bin bags in the boot of the car so you have materials to hand if the shops do not wrap it up for you. Do not have stuff posted to you where it will attract attention of the post office.

Stuff for the action should be handled with gloves and cleaned of fingerprints using white spirits or washing up liquid. This should be done when they are acquired, and all identifying labels removed and destroyed. Give them another clean before leaving for the action. Keep gloves available so they are there when you do need to handle cleaned material – is all too easy to slip up on this one, and you can just as easily drop DNA as fingerprints.

4.6 Clothing & other traceable

During the action itself, you will leave a number of trails behind which forensics can be used to investigate. For a good introduction into DNA forensics check out the GeneWatch report at
http://www.genewatch.org/HumanGen/Publications/Reports/NationalDNADatabase.pdf

4.6.1 Footwear

Shoes and other footwear all leave distinctive marks; cuts and wearing in the treads can be used to identify your shoes as the ones leaving a trail. This is an issue if you are going to be in an area with mud or you have to cross it. Buy disposable pairs or put

socks (which will pull up high) over the top of them, with a plastic bag between the outer sock and the footwear, so when you come to take the muddy socks off, you can do it in a clean sweep and bag up the mud and dirty outer socks in one go without getting it on your hands or cloths either.

Tip: If in the field always plan in case of getting mud on the rest of your clothes, especially your trousers. If you have to leg it as part of a get away it may single you out in a town environment.

If stopped on the way out, an old trick was for everyone to take off their shoes and socks (shoes can linked to socks through fibres) so individual pairs couldn't be identified with anyone in particular. Modern forensics could probably work this out, but it is expensive and whether they put that amount of effort in will come down to how badly they want you.

If they are muddy, wash it off if possible, and have newspapers down in the vehicle to catch it.

Note
[a] In the UK impressions of footwear can now be taken at the roadside by the police during car searches.
[b] Glass shards is another tell-tale sign on shoes and used to place you at a scene.

4.6.2 Clothes
Depends considerably on the action. Nondescript is best, and the closer everyone dresses the harder it is for individuals to be singled out. But consider the context and your aims – a load of people wearing heavy black outfits trying to sneak through town is going to stand out. It is more important to dress for what you want to achieve than to fit in with your group; for example, camouflage gear is not always the best.

I. Black is not always the best colour, for instance getting caught in a field of snow. Consider grey or khaki. In our experience charcoal grey works best in general for not standing out in a field, etc.

II. Avoid clothes made of nylon (very noisy when you move) but go for clothes which are lightweight and comfortable as a general rule – often the adrenalin rush will keep you warm, but consider if there will be much waiting around to do.

III. Zips are also noisy and buttons are preferable.

IV. Make sure you have nothing reflective on you (unless it helps you blend in).

V. If doing an action in town or where you may be chased, have a different coloured layer underneath to give you a quick change of appearance – examples are bright T-shirts or a reversible coat. Or a different baseball hat.

VI. Clothes can be used to disguise your shape as well, so go for baggy clothes which create an asexual figure.

VII. Keep your hair and facial features hidden. Hoods & baseball caps are good, as are masks and balaclavas. However this depends on the situation, as sometimes wearing masks and balaclavas are just too much of a give-away. Snoods are good as they can be quite obscuring, and they are a legitimate clothing item. Ski-masks are not as good as they can give away too much facial features around the eyes.

4.6.3 Hair
Wash your hair and give it a good brush before leaving on the action, so no stray hairs fall out. Keep it tied back and out of the way.

The alternative of providing the forensics team with no information at all is to provide them with too much information by deliberate contamination. A technique used by some is to gather hair from the floor of a hairdressers – pose as an artist – and put that in your balaclava, etc which may have to be discarded. The result with be a nightmare for forensic, if down right impossible to prove anything with. The same goes for gloves as DNA can now be extracted from the inside of hats and gloves.

4.6.4 Fingerprints
Wear gloves where ever possible. Be aware that latex ones can still leave an impression. Practise using any tools with them so you are comfortable with the sensation and the change in grips.

If gloves slip or are impractical, remember to wipe down every surface you touch, including palm prints – forensics look at the entire hand as opposed to just the tips of the fingers. Have scraps of material soaked in white spirit ready in a bag (sealed to stop it evaporating).

4.6.5 Maps

Essential but with pitfalls. A map found on you or nearby the event with markings on it and your fingerprints is can amount to pretty convincing evidence. Markings can be as simple as a lot of fingerprints over the relevant spots.

Techniques to use with maps are

e. Do not use markings that cannot be easily erased – this goes for pencils which leave indentations even after being erased.
f. Use laminated maps where tell-tale marks can be wiped quickly and more securely and don't have as big an issue with fingerprints as paper.
g. If in doubt, buy new ones with easy wipe covers and use gloves.

Don't print off a map of the site you are visiting from your home computer, instead use an Internet café to do this.

4.6.6 Other materials

It is good policy to remove any unnecessary items from your clothes before you leave to go on the action. Anything that can fall out of your pocket could end up being traced to you through forensics. Don't bring ID, things that rattle, etc; take only the keys you need and not the full key ring. Though bring some change for phone calls.

Tip 1: Keep personal items you need in a zip-up pocket, and always separate from anything you need for the action.

Tip 2: Use torches with a red gel over them for outside work – the light does not carry near as far.

4.6.7 The Vehicle

You want to keep this as clean as possible, especially if it is a hire car. Techniques to use are

- Use plastic covers on the seats.
- Put down newspapers
- Have cleaning materials ready in advance, especially for transit vans. This includes black bin bags for disposing of the newspapers, etc.
- Have materials to wash mud of the side of the vehicle (clays can be used to pinpoint where you've been).

There are reasons for this. Even if they trace the vehicle, you don't want to leave markings in it that may be used against you, or ruin alibis for having it. Nor do you want to leave memories of mud, etc. in the mind of the rental company.

Everyone should take charge of ensuring the vehicle is cleaned, and it should not be left down to the person who hired it.

4.7 Disposing of Equipment/Clothes

This is something you should budget time and preparation for. It is often forgotten about, but is crucial as to getting away with your action.

Anything that may compromise you should be burned or otherwise securely disposed of. Dumping them in a river/bin a few miles down the road may not be enough. The more severe the action, the more they are going to put effort into searching for stuff. That something was expensive should not be an overriding excuse to keep it if there are other risk concerns.

Don't keep stuff to 'recycle'/reuse if it is distinctive or you cannot justify their presence in your house. Some stuff is not illegal in itself so they still need to prove that you used it for the action and had no other reason for having it. For example, keeping tools in the tool shed. If in doubt take the more cautious approach.

Souvenirs of an action are a very bad idea. People can get quite silly over this, so this needs to be spelt out in advance.

Clean vehicles thoroughly; wash them down and use disinfectant if necessary, so that even if they do trace the vehicle there will be as little as possible evidence in it. Budget enough time for this as it can be a bigger task than realised.

If you are keeping equipment wash it down thoroughly using soapy water or white spirits.

Bolt-croppers and such like can acquire tell-tale scratch marks on the blades that link them to the action. They may as a result need to be filed down. If you are planning to do this, buy the material in advance and not after the action.

If you are leaving with equipment people in the vehicle can help by filing down tell-tale marks, wiping stuff clean and general helping with the disposal process. Include the clean up material in the list of material to bring on the action or to have at your base – eg. cloths soaked in white spirit, filing tools, working lighters, bin bags & cleaning agents.

Where clothes and equipment are being physically destroyed, then don't do it either near the site of the action or your homes. The farther away from both of them the better, depending on the nature of the action.

People have been caught because they simply tossed spray cans, bottles, etc into nearby bins and gardens, whereas if they had taken the time to put some distance between them they could have been disposed of innocuously enough, even with fingerprints on them.

4.8 Communiqués & Photos

Make sure you can send these securely; if it will compromise you, then don't send them. Consider waiting a while so the heat drops down. Never do it from your home, and avoid using your town if you can – the greater the distance the better (relative to the seriousness of the communiqué), and avoid CCTV were you can.

Be careful that nothing in the text gives you away: if in doubt leave it out.

Eyes should be blocked out in photos, even if masks, etc are worn. Consider when using pictures of backgrounds that you might want to avoid features that can be used to locate the place, or if they come looking at the place they can match it up with a published photo – use sheets as a backdrop. Sheets with slogans on them can be evidence if people are unfortunate to have unwelcome visitors who find them and make the association with the photos.

4.9 Mobile Phones

See the separate briefing for a guide to using mobile phones securely.

If they are required for a covert action, we suggest that you purchase a set of phones with no connection to any known activists. Once a phone is used to ring a number outside of this small network, it is compromised. They should not be used until the day of the action (other than to charge batteries) at which point they are taken somewhere private (certainly away from activists dwellings) and prepared. In some situations it is advantageous to put the numbers of each on phone so you can speed-dial.

Once the need for the phone is over take the battery out, and appropriately dispose of.

4.10 Phone Boxes

Phone boxes are still a pretty good ways of making anonymous calls, though they do have pitfalls you need to be careful of. To avoid them we suggest the following guidelines:

1. The use of phone boxes should be varied as much as possible. If a phone box (or even several specific ones) becomes identified as one being regularly used by activists for communication then a camera may be put on it. People have been convicted as a result of this.

2. Use as far as possible from your house/office – cycling to other villages/estates is good.

3. Avoid areas were phones are likely to be already monitored, such as town centres where there is already much CCTV or areas of high drug dealing. A simple bug scanner will often pick up if there is a camera monitoring it by picking up on the camera's transmissions back to base.

4. Wear baseball caps & non-distinctive clothing. Keep your head down. If you can, slip a mask up on (in case of pinhole cameras in the phone box), put not at the expense of making you stand out to passers-by.

5. Use gloves to handle the receiver and depending on what you are saying, consider putting a *clean* cloth over the microphone part to stop leaving traces of spit, and to disguise the voice.

6. Phone box to phone box calls are not secure; in fact they are seen as a trigger for state monitoring.

7. Phones in hotels, bars, etc are also useful sources to make phone calls from.

In the UK it is possible to type in 141 before dialling the number for your call. In theory will anonymize your call so that the person at the other end cannot see the number. This is no longer always the case with the introduction of new technology to defeat nuisance calls. However, for many numbers, especially ones not commonly targeted it will still work.

It should not been seen as a measure guaranteeing security but as adding an extra layer of security. For actions we do not recommend this approach as you should not be doing stuff from your home phone line at all, but if your level of risk is very low then you can consider this approach. Otherwise, this should not be crossing your mind. It may be more applicable if you are doing campaign administration stuff rather than actions, though in this case you should consider a system where your phone number is automatically blocked.

4.11 CCTV

CCTV is everywhere these days, but not impossible to hide from. Learn to recognise the various types of CCTV there are, but also be aware that they can be in shops videoing what passes by the windows. For an idea of what the less obvious types look like check out http://www.brickhousesecurity.com/cctv-security-cameras.html. Quality does vary considerably on cameras, and some are decoys, so often they are there simply to act as a deterrent more than anything else.

A camera with a red light generally means that it has infra-red/night vision. Increasingly, CCTVs in cities are also being fitted with microphones, and conversations can be tracked down streets.

CCTV also allows investigators to pick up on body language so no distinctive slouches or swaggers – keep to an ordinary straight backed walk.

A good site for dealing with recognising and dealing with CCTV is http://www.rtmark.com/cctv/

Avoid looking up while doing your shopping, wear baseball caps (without distinctive markings) for good cover. On actions, what matters more is whether there is a security guard present, as most CCTV is time lapse recording to be monitored later, so if you are masked up then it is of little consequence.

Tip 1: when escaping down a street, do not take off covering cloths until you are sure you are out of sight of CCTV, unless it is going to be too obvious, such as making your escape into a busy area of town.

Tip 2: Put masks on before getting out of vehicles; and leave them on for the duration of the action (avoid taking them off to scratch itches).

Tip 3: Masks can itch or steam up glasses; so practise wearing one before going on an action so you know if it is going to cause problems.

4.12 Travelling

When driving, pick country roads and motorways, avoiding towns as much as possible as that is where the greatest concentration of camera is found. Keep within the speed limit to avoid being stopped by police for speeding and setting of speed cameras. If you are in a hire vehicle – recommended – then you will be safer, as police vehicles now have cameras connected up to computers which can capture your number plate as you pass and let the police know if the vehicle belongs to known activists.

The best times to travel at night are around pub closing hours and after 4 am. This way you fit in with the flow of traffic. Some activists avoid travelling between 11.30 and 4 am, depending on the nature of the action – suggesting instead parking in a wood or similar and sleeping until it was time to travel again. Beware of smoking if it is not an appropriate place.

If the police are alerted immediately after the action there may not be time to get out of the area, especially if you have a distance to go, so again you should consider if you should be on the roads at all as you may be more likely to be stopped in spot checks. This is a hard call, and the difference between fleeing the area and hiding it out will differ greatly from action to action.

If you do get stopped have a blag story ready – say you are on your way to a party, or something believable. Being dressed to look like trouble will only invite further curiosity from any police who spot you passing. One technique is to have two people in the front who look smart, ideally a man and a woman, with everyone else lying down in the back a you travel.

If you are stopped, don't panic – they may not have the evidence you committed a crime depending on the situation. It is good to plan in advance what to do if this situation does arise.

Something worth noting is that some hire companies have tracking and GPS devices on their vehicles to record where it has been. This may not be an issue if they are not going to trace back to the hire company though and it has been hired well away from where the activists are based.

Tip: Do not bring your mobile phone along as it can also be a tracking device.

A new development is Automatic Number Plate Recognition [ANPR]. This technology allows police to monitor passing vehicles with a camera and process the number-plates with a computer. If a number-plate is recognised as belonging to say a stolen vehicle or a car belonging to a known activist, then the police may stop the vehicle. Currently these cameras are mounted in police vehicles. However, the Government is currently rolling out a scheme to convert traffic camera to have ANPR, with the data being recorded at a site in Hendon. Petrol stations and supermarkets are also being brought into this network. This will allow them to record every vehicle which will allow them to analyse journeys made over several years if necessary. More information on this is at http://news.independent.co.uk/uk/transport/article334686.ece

This will only work on legitimate number-plates, and will not have any effect on bikes and possibly not on vehicles innocuously registered, or not registered at all. It can also be partially avoided by travelling on country roads where there are less such cameras.

4.13 Being chased

It may happen that you pick up a police tail while leaving a covert action. Depending on the action, you may either decide to accept the fact. However, if the consequences are serious, it may be worth trying to lose it. However difficult it is, keep your cool until you are certain that the police are onto you – more often than not it has been possible to talk your way out of it.

4.13.1 On foot

Scatter in groups of between two and three, preferably matched by speed. Solidarity is all very nice, but there is no point everyone getting caught. Been matched by speed means you are not too spread out making you easier to spot – tight groups are better when moving through the countryside at night, as they stop people behind blundering into situations and reduce the ease of being spotted. Keep your attention on moving and not discussing what went right/wrong.

Different groups should move in different directions; you do not want to be leading the police to another group of you. When doing preparation for an action run through routes to the rendezvous point (at least one person should have actually made it so knows of any issues not identifiable on maps or of other dangers.

Always have a secondary rendezvous and time in case this is necessary. In this case people should have maps of the area (no markings) and/or be familiar with where they are and what they are looking for. There should also be a time limit on how any pick-up vehicle will wait to pick-up; again this is about not jeopardising others who have already arrived by hanging around until you attract attention.

Tip: if you arrive early then waiting hidden until the pick up vehicle arrives. Check that they have not been followed before you show yourself.

Hiding may require you to keep your cool especially when there is someone standing quite literally over you. Gardens, woods and hedgerows are all good for ducking into. The key is to relax and keep control of your imagination, for example about just what is crawling up your leg. Itches are a nuisance but easily conquered with a bit of practise: they are always at the worst just before they disappear and the desperation to scratch is at its highest. In some cases actively focusing on them does the same job. Also remember that in this situation your sense of time becomes greatly distorted, normally much less time has passed than you think.

4.13.2 In the car

If you are certain that it is the police and not others who are onto you, you have nothing to loose – the chances are that the driver will cop it anyway, but passengers still have a chance. Try and locate somewhere you can jump out of the car and leg it. If you are getting chased by workers or others who are likely to inflict violence on you, then you need to attempt to evade them. We will not go into more detail on that here, but a search on “escape and evasion driving/techniques” or “emergency high speed driving techniques” on the Internet should provide techniques for evade cars attempting with would-be attackers.

4.13.3 Abandoning the car

If the car has to be abandoned, so be it. The people to whom it is registered to or who have hired it will still have to deal with the investigation so if they are not present they need to informed that this has happened, but watch out for late night phone calls that make them suspects – consider having a system where a specific number of rings means trouble, but that they do not answer it. Remember to us a payphone or clean mobile phone and not one of the action mobiles. There may also be DNA left in the car that will implicate the driver and passengers, but this will take time to be followed up. This situation can lead to increased monitoring of suspects for a while in the hope of finding more direct evidence. Be prepared for this but avoid raising more suspicions.

Of course, it may be that the car is registered to an address or organisation so that the people in charge of it cannot be immediately identified; or it may be the case that the car is stolen or newly purchased so that the registered owner is not fully aware of it being used in the action (such as one recently bought and the documents have yet to sent off or processed by the Licensing Agency). Where this approach falls down is if the car is already known to investigators who have you under surveillance so know you have access to it. The chances are that the driver will still be caught.

Some activists have effectively false number plates to throw investigators attempting to trace the car. The often try to match the replacement number plates from a similar make and colour of car to the ones used on actions, so automatic number plate recognition monitoring does not trigger any alerts (eg wrong type of car or non-existing number plate. Vehicles also have chassis numbers and other serial numbers which can be used to trace the identity and history of the car should it be found abandoned, even if it has been burned out – though they are unlikely to go to this amount of trouble unless they are pretty determined to get the activists, and even then it may not actually lead to a chain of evidence. Burning out the car will, however, get rid of DNA evidence.

Disclaimer: we do not condone any of these approaches, and provided as an information service only. Modifying a car's license plates is illegal. We encourage people to avoid breaking the law. Just so you know.

4.14 Evidence gathering tools

Directional microphones can pick up conversations even if done from a helicopter, so avoid discussing things on demonstrations and when discussing things of a highly sensitive nature, take great care of where you do it, if this sort of surveillance is a risk.

It is the same with cameras. They do not need to be mounted directly outside of your house/work to be watching you, and sometimes the houses of neighbours are used.

4.15 Debriefing

A useful thing to do for a variety of reasons, though security should be as tight as for planning meetings.

IX. Go through what went right and wrong so you learn from mistakes and improve for future actions. It is important to be honest with yourselves in order to learn from mistake, though avoid attacking each other or putting blame on people for what was bad luck as that destroys group morale. A good debrief will help people grow as activists and/or show where people are better deployed in future actions.

X. With what went wrong, consider where there are people now at risk and what can be done. It should not reasonable or useful to expect everyone to take the fall in solidarity with one person unless there exists a prior agreement to do this. However, it is important to arrange support for those potentially taking a fall so they are not left feeling isolated which could leave them vulnerable to breaking or dropping out of the movement.

XI. To remind people not to talk about the action, especially with others not involved. People will want to discuss the action, especially if it has been very successful – it is a part of human nature. A debrief gives people a chance to deal with this so making it less likely for them to talk to others. If someone feels the need to talk further they should not do it with anyone not involved in the action, but arrange a meeting with another member of the group.

XII. Remaining responsibilities to deal with should have already been planned for, but unforeseen circumstances may have cropped up requiring further decision. However, some degree of freedom for different group members to do the jobs allocated to them should be in place. With luck this part of the process should be a matter of simply checking off jobs done.

4.16 Shitting in your backyard

This is a phrase commonly used by experienced activists. And also by paranoid people as an excuse not to do small actions near them.

It is useful advice but it needs some interpretation. Basically it is not about bring attention to yourself on several levels. One level is covering the environs around your house with loads of political stickers, graffiti, etc as that just marks out the area as somewhere to watch and makes it easy for them to find you.

It doesn't mean you cannot do actions in and around your town; just don't make it obvious it is centred around one particular street or area.

On another level, it refers to actions with significant consequences and which may even lead to raids. Action with these sorts of risks should not be carried out near where you live. Yes, it may be frustrating to live down the road from a particularly evil company, but if you are going to do something drastic to it, then you will be the first one they will focus on. Small scale stuff is not so much an issue, but the larger scale stuff is.

If company X has a factory in your town and someone spray paints the wall or glues the locks, then the most that may happen (if they don't catch the perpetrator straight away or find their equipment) is personal calls by police trying to find people willing to talk or to rattle peoples cages. In fact it is a good sign if they do this, as it shows that in reality they have little to go on. However, in serious cases, where say someone from a more hard-line group attempts to burn down the factory, then the known activists in the immediate area will find themselves under much more scrutiny and doors may be kicked through in some cases. This is essentially a knee-jerk reaction by police desperate to find evidence. However, if the perpetrator is not from the area they have much less chance of getting caught.

At some point you are going to make value judgements and go ahead with the risks. People have got away with surprising amounts of stuff relatively close to them by taking the right precautions; however, as a rule of thumb, interpret your 'backyard' as

The more serious the consequences of an action the further away
from your home you should be doing it.

4.17 Conclusion

There is a lot of material in this section, and a lot will not be applicable in every situation. Work out what your security needs are and what applies to you and your actions. For example, if you are organising a straightforward demo, you do not have that much to fear and a lot is inconsequential; consider about making life as difficult as possible for anyone investigating, but not to the point where the demo becomes impractical. For example, you don't need to set up closed phone networks for a demo, but you can throw a spanner in the works by using unregistered mobile phones or payphones.

Remember, that protecting your privacy and not leaving DNA/fingerprints is not illegal…

5. Security for Demonstrations

If you are a person involved in covert activity consider whether attending public protests is necessary, since you want to be bringing as little attention to yourself as possible.

Demonstrations are fluid things and it is impossible to guarantee they will go off as planned. You need to know your law, and if you are going down with an affinity group then you need to go over the various consequences that may arise in case of trouble, such as prisoner support, and what behaviour is expected of the group on the day. There is no point causing a split in the group because one section felt uninformed or unready to deal with the actions of another section.

5.1 General rules for demonstrations of all types:

h. Avoid calling out peoples names; use pre-arranged nicknames or generic shouts.
i. Do not make it appear if one person is more significant than others; group discussions should be done as a group, not one person going around asking individuals.
j. Never discuss plans at a protest or hold meetings around them. Demonstrations sound noisy, but directional microphones can easily pick up conversations – including from helicopters.
k. Under UK law masks can be confiscated under Section 60AA, though that does not make them illegal as such; however, the police are just as likely to say that you are attempting to be intimidating and harassing by wearing one. Baseball hats and coats with high collars can also hide the face, as can holding up banners in front of you.
l. You never know who is around you at a demo, listening in or just watching you to make a wrong move. It is well documented that police will send a large group of people into a crowd where they will incite and/or monitor so at the end of the day you may find yourself suddenly arrested by someone who had spent the day next to you and looked like a fellow protestor.
m. Avoid carrying ID in case you are stopped and searched – police will do this as much to collect intelligence on who is going on protests; though if you get arrested and cannot confirm your identity then they may use this to keep you in the police station for longer.
n. Keep an eye on exits from the protest, so you can leave fast if need be.

5.2 Evidence gatherers (EGs) / Forward Intelligence Teams (FIT)

Demonstrations attract police intelligence teams like flies. What they are interested in is recording your presence, any clothes that can be used to identify you, and most importantly who you are with or talking to so they can build up their profile on you. If you don't want to be associated with another activist publicly then don't be seen talking to them at public protests.

Another function of these particular police is to intimidate through constant photographing/videoing. Some times they are deliberately intrusive into people's faces and activities as a way of winding people up and so they can demonstrate their own power.

5.2 Cameras

Photograph/video people acting suspiciously, rough behaviour by the police and any arrests they make. Once this is done, take the memory card or film out immediately and pass it to someone else. Put in replacements. If the police see people photograph their illegal actions they have been known to target the photographer and destroy the evidence.

Avoid taking photographs of fellow activists, especially stuff that may compromise them. It is great to have action footage, but not at the cost of someone's freedom. Always respect requests to stop using camera, and never assume that you have an automatic right to video. If in doubt ask first.

In the UK the police have the right to seize cameras if they thing they contain evidence, a power they've been known to abuse.

5.3 Travelling to demonstrations

If a car is stopped on the way to or from a protest, look away to hide faces. If passing a police vehicle, duck down so they do not realise that it is a car full of activists – often they are on the look out for vehicles packed with young people to stop and search. However, with an increased use of automatic number-plate recognition technology there is a tendency to focus on known activists vehicles. If the vehicle you are in regularly goes on protests then it is far more likely to be stopped.

Likewise, consider if putting up posters on your car windows whether it will be drawing unnecessary attention to it, especially if they are left up while the car is parked up. This is not to say don't do it, but if you are up to something you do not want to draw attention to or are in a vehicle with an increased chance of being stopped, then do not make yourself too obvious.

Try to avoid going to and leaving a demonstration by oneself as you leave yourself open to being harassed by the police who see it as an opportunity to intimidate you from going to further protests or as a way of arresting you out of sight of witnesses.

5.4 Debriefing

If a protest does not go as planned and there is a heavy-handed reaction from the authorities, it is good for people to debrief afterwards, even if it is only in the affinity groups where it can help people understand each others reactions. This is important psychologically, and for being able to work together should similar events happen again. Violence can have hidden psychological effects that find release in drugs and alcohol consumption or depression if not dealt with by discussion.

If people are suffering from depression or other fall-out from assault or other issues following on from a protest turned violent by the state, then it is important they are looked out for and helped. This is as valuable a prisoner support, and people should not be looked down upon for feeling bad about a situation out of their control. The Activist Trauma group is a grassroots network which exists to help people suffering all forms of trauma – for more information visit www.activist-trauma.net

5.5 First Aid

The state and other opponents can resort to violence, so it important that there are people around with first aid training. There are groups offering free training and online resources so check them out. Depending on the nature of your group's activities, consider paying for someone reliable to be trained up, and ensure that they are not put in positions where they are unable to help others. This is particularly useful if you are engaged in confrontational actions or hunt sabbing. Another use of first aid is how to deal with tear gas or pepper/CS sprays.

In the UK, the Action Medics group (www.actionmedics.org.uk) provide first aid training for activists, and are often present on the larger mass actions.

Self-defence training will also teach you how to take and/or deflect blows so they do not do as much damage. Often what you need to know is simply how to hit effectively so you can get a good head start when running away from a potentially violent situation.

5.6 Dealing with Provocateurs

If you see someone inflaming a situation beyond where you are willing to go, then get out of there. If you are confident that someone is a provocateur then call them out, but beware what consequences your actions may have, especially if the crowd's mood turns ugly.

Do, however, alert people around you and get people to photograph their actions as this may help genuine activists when the come to court.

If you don't feel confident about outing the provocateur, consider following them discretely, and photograph them, especially if they are later seen talking to police or even getting into a police van. Then let campaigns know as it may help other people's court cases.

Infiltrators have been known to attend demonstrations, both to stir up trouble, justifying police oppression, and also to gain reputation that is useful for worming their way into other groups.

6. Personal Security

As with all security, tailor your needs to your actions. There is no need to go to extreme lengths if that is not called for. If you only do very fluffy actions and hang out with like-minded people, you only need basic security, do not need to implement every measure possible. If you are doing covert actions, then you need to take much more effort.

A rule of thumb is that the higher the risk, the lower the profile you want to have. For example, if involved in covert stuff, you do not want to be attending demos or getting involved in public disorder situations where arrests may lead to your house being raided, or simply more attention is turned onto you. Dating high profile people does not help either – think about where your priorities are. The lower your public profile the less chance you have of appearing on the state's radar and encourage investigation of yourself.

A mistake well known activists can make is to disappear suddenly from the scene, while remaining in contact with other activists: it sets alarm bells ringing. If you are going to disappear underground do it gradually.

The main threat to your security is how much of a profile they can build on you and your network of contacts. The police regularly monitor new people on a scene or in a known active group so they have an idea of who they are and whether they deserve further attention. This basic monitoring is routine, and people often make the mistake of noticing it and immediately assuming that they are in trouble or their door is about to go through any moment. The reality is that you have just appeared on their radar and they are doing a bit of background research to find out more about you for the future.

Another reason for carrying out surveillance is to confirm information that they have received from other sources, such as phone taps and grasses. For example, that you really are on the way to a family funeral, and that it is not code for an action. Other reasons are basic information gathering – they may be sat outside your house simply to find out who your friends are so they can build up their profile on you and the groups you are in.

It is unnerving when it first happens to you, but keep your cool, don't do anything rash, just be aware of the situation. Panic only gives the impression you have something to hide so draws more attention to you.

Knowing that you're under surveillance or that your house may be bugged may have a psychological effect. It is a horrible intrusion on your sense of space and personal life. Don't bottle it up as that makes the paranoia worse. Talk it out with fellow activists and work out ways of dealing with it. It is good to remember that you are being bugged and under surveillance because you are been successful and being successful is what counts. Also if you play it right it is possible to outwit them.

6.1 Dealing with the police

The police, in our experience know less than they pretend to. We have found it much easier to expect them to know something but not to let it rattle us if they use it.

A common trick is to use your first name, or to deliberately let slip some personal detail about you into conversation. When you think about it the information is often pretty innocuous, and simply shows they have been doing some background checking – frankly, so what? Ask yourself, why are they doing this? Why else would they admit they've been checking up on you, and basically doing their job, unless they want to rattle you? If they were doing a proper surveillance job on you, they are not going to be letting things like that slip. Rather they are either trying to frighten you off through paranoia, or scaring you into making a mistake. Stay cool, don't get rattled and evaluate just what it mean in the light of what you plan to do as an activist. In our experience, it generally amounts to very little.

The state is looking for two main things about you: your beliefs and your network of contacts. That is, what are you up for doing, and who are you likely to be doing it with. State intelligence is not generally directed at solving a particular crime but at building up a database of knowledge, so that when something does happen they know where to look straight away before the evidence has time to be destroyed.

Evidence gatherers at demonstrations are a common feature, and people get quite nervous about their constant photographing of people. However, if they were simply recording your presence there, they'd only need one photograph. What they are looking for is who is doing the speeches (in their eyes an indicator someone is a form of organizer) and who is talking to whom. It is the latter they are most interested in, as it allows the network to be built up of who is friendly with whom. Next time you are on a demo, watch the way they move and work; look at the people they are photographing and what they are doing.

On a personal level, your opponents are just as prejudiced as the rest of society in stereotyping on how people dress. If you wear radical t-shirts supporting underground groups or provocative political slogans or a dressed in quasi-combat (to project a 'hard' or 'activist' image) or 'punk' clothing, you will to stand out.

Clothing and appearance is important, but if you are going to be a serious activist, standing out is something you should avoid. It is nice to be an 'individual', but if you are doing stuff which attracts state attention why help them mark yourself out? Unfortunately, we do not live in a utopia so activists serious about what they do, will have to make this sacrifice. The idea is to blend into the society around you. Dress causally in everyday clothes with 'normal' hair as if you were an 'everyday' member of society. It is all very well to debate the nature of what is 'everyday' and 'normality', but the reality for a covert activist is that the stereotypes are generally quite clear; these debates should be put aside for the practical reality. Your aim is to get away and continue being active, not bringing attention to yourself but to your cause.

A person with a green mohican is very easy to follow around. Even wearing a distinctive jacket everyday is enough to mark you out, and make you much easier to follow. Describing regular clothes worn is much easier to do than to describe faces unless there are other distinguishing features (beards/particular glasses/hair style).

If the state does mount a serious surveillance operation against you, the chances are that you are not going to know. However, a common mistake of the paranoid is that this goes on against everyone all the time. The state simply does not have this sort of resource – that sort of budget is kept for the people they see as genuine threats which in turn comes from studying their previous intelligence and from inside information. Unless they are really out to get you, you are more likely to be targeted intermittently so they can update their files on you, and by low-level coppers who give themselves away to the prepared eye.

Being approached to be an informer is always a possibility and should not be discounted even of very seasoned activists. For what to do if you are approached by the police we recommend the article on the freeB.E.A.G.L.E.S. website at http://www.freebeagles.org/articles/grass.html

6.2 At Home

Below are some techniques and advice for protecting yourself at home. The way to approach it is to ask yourself, "If the police came in now, what would they find which would put me at risk?"

The other rule of thumb is to never discuss anything sensitive in your house. Going out into the garden to discuss stuff is not safe either. Even if they have not bugged you, don't take the risk of letting them know what you or others are up to.

If someone calls around to let you know about an up coming action or to arrange a meeting to discuss a sensitive issue take a walk, preferably in a direction you don't normally take. If you use the same route regularly for sensitive discussions consider changing it. Leave mobile phones in the house.

6.2.1 Control the information in your house

Burn your rubbish, personal letters & bills. These contain a lot of useful information about you, your habits and your contacts. Have a process where you do not leave stuff such as envelopes, notes, samples of your handwriting, etc lying around, where a grass close to you could read or pilfer. For example, if you are in the habit of noting mobile phone numbers or email addresses down on scraps of paper gather them up regularly and destroy.

Depending on your background, situation and the nature of your activity, consider whether having any radical literature is necessary to be there. If you are not well known or acting independently, this sort of material is valuable evidence showing you have interest in the movement/campaign/etc.

Diaries are a bad thing, even if well hidden. If you think of a good hiding place, you can be sure that you are not going to have been the only one and that people who specialise investigations are also going to be aware of it. This includes behind pictures, under boards, in cisterns, tapped under cupboards, inside cushions, etc.

Saying that, if it is a raid by low-level coppers then there is a good chance they will over look stuff – certainly we have heard enough stories of police missing the obvious. What you need to do is consider the balance of outcomes – how likely you are to be raided by the sort of agents of the state who know what they are doing, against the risk that information is to yourself.

Any risky information should be put on a computer disk and encrypted using PGP and stashed, so at least you have a chance of keeping the information out of their hands even if they get the computer or disks.

Do not give your car keys or house keys to other people unless you particularly trust them.

6.2.2 Preparing for a raid

If you suspect that you are going to be raided at some stage – for example an action has gone wrong, or something big has happened in your area so the state is being very inquisitive - keep all sensitive material in your house together so that if you have to remove it in a hurry, you are not wasting time searching for that elusive but damning piece of paper. Planning a process to deal with the risky information in your house will make this much easier; it helps prevent you loosing material and gives you a greater degree of control over it.

Remember, if you are being watched any panicky action will be noted, thus bringing further attention yourself. This is one reason why police knock on activist doors – they may know you are not going to tell them anything, but if they can rattle your cage enough so that you slip up then they may be able to get something on you.

Tip: If you do get a visit do not start ringing people involved in your action or similar, as the phone calls made after a visit will receive more scrutiny and may indicate other people as being worthy of attention.

Sensitive material should be removed from your house on a regular basis in a calm manner – not furtively! This does not prevent you from practising counter-surveillance techniques, but do so discretely. Any sensitive material (including anything relating to the target, even if it is simply leaflets on related issues) should be dealt with before an action, not after. This goes for simple stuff as well – a magazine from Greenpeace can and will be produced as evidence to show that you are interested in anti-GM issues and inferences can be drawn from it, especially if your target happens to be mentioned in it.

If you get wind that something has happened and you suspect you may get a visit as a result, stay calm and prioritise what you need to get out of your house. Get friends to call around and take stuff out for you, or 'take back their possessions'. Again planning for such events and having safe places set up will make all this easier to deal with on the day – in the middle of surveillance and knocks on the door is leaving it to late, and you will not think as clearly – plus your contacts will not be pleased at the sudden attention you may be bringing unannounced on them.

Depending on your location, you may actually be able to leg it – as in one case where one activist in a house about to be raided grabbed the computer and legged it into neighbouring gardens, getting out of the area safely.

Even if you don't have anything to worry about, material-wise, in your house, the attention from the police is unsettling. Often (though unfortunately not always), such visits are simply to rattle and intimidate you; as such they should be treated more as a statement about the level of their intelligence and the evidence they had. If their intelligence was particularly good they wouldn't be stopping by to see you for a friendly chat, but dragging you to the police station for a less friendly one.

If you allow it to panic you into paranoia or ineffectiveness, then you have let them win. There are activists who are raided almost on a regular basis, who still continue on doing very effective actions.

6.2.3 Phones, computers & emails

Clicking and whirring sounds or feedback on your phones does not mean you are being listened though, though it may be that they are intending to induce a sense of paranoia. The reality is that if they want to listen to your conversations you are not going to know about it. The same is true for emails and mobile phones. Basically, never say anything on the phone you would not be prepared to stand up in court and admit. Never plan anything over the phone you would not want your opponents to learn of. When preparing an action, remind even experienced activists in case that it is not clear how covert the action is to be. If you are reminded do not be offended, it is just good practise and nobody is perfect.

Even if what you are saying is not illegal in itself, think about how much it could be used to build up a picture of you and others which would be useful to their profiling of activists.

Any phone can be converted into a listening device that can be activated remotely, and the ability to do it has been around since phones were first developed. If you are having a sensitive conversation you should not be doing it in a room with a phone in it, land line or mobile alike. Whispering on the phone does not work!

Places like GCHQ in Cheltenham monitor every phone, text and email communication. This is achieved by sophisticated programmes that do more than pick up on key words, but also put them into context. It is not infallible, but it is something to be aware of. Using codes can work, though in our experience they will sometimes check up these cover stories. The best advice is to avoid planning stuff over the phone and email depending on the seriousness of the activity.

Some activists recommend using a programme called Skype, if you have broadband, to make phone calls. This uses the internet to make your phonecalls using what is known as "VoIP". Its main usefulness is that you do not have a phone bill listing the numbers you have been calling. Later versions also use encryption software for Skype to Skype phone-calls which is apparently causing security services headaches as it means that even if they can not use the Skype calls in a court case they cannot listen in for intelligence gathering purposes. See http://www.theregister.co.uk/2007/11/23/skype_stumps_german_spys/ and http://www.theregister.co.uk/2008/01/29/skype_trojan/ for futher discussion of these issues.

However, there are several criticisms which limit Skype as being a more useful security tool for communication. There is evidence emerging that Skype to land-line calls (using something called Session Initiation Protocol or SIP) can be eavesdropped on. Another problem is that the Skype software is not open so without peer review of the internal code one can never be certain that it does not contain various flaws which others can exploit to listen in. We know that software companies have put

back-doors into their software at the request of governments so we would mark this up as serious concern, as various computer security experts have raised.

The problem with this sort of approach in general is that it will not defeat bugs in your house or on your computer. It is, we recommend, a useful tool for low-level security that hampers their efforts to build up a profile of you (plus being cheaper), but we would not rely on it for anything a higher level of secrecy.

It is a truism that the more you rely on technology the more that the flaws in it open you up to monitoring not just by the state, but by other groups/individuals as well who are unlikely to be working from the best of motives.

With regards to email, unless you encrypt it properly it is not hard at all for it to be intercepted and used against you. Ideally you will be using GPG encryption with Thunderbird email programme on an Ubuntu/Linux desktop, and ignoring Windows/Outlook altogether.

While the phone and email are useful for facilitating and initiating stuff, but they do have their limitations. It is possible to make email more secure through various techniques, but you have to be proactive about introducing them. See below for a chapters on mobile phone security and touching on securing email.

6.2.4 Mail

Mail is easily opened and read. Some times it is done very obviously, other times not. One sign to watch out for is mail appearing in a bundle every few days. Another is regular tears on the flaps.

When sending mail, glue or Sellotape down the corners of the envelope so it is harder to tease the letters out (done by using tweezers to wrap the letter into a thin tube that can be pulled out. Also secure other seals on the letter so they cannot be steamed open. Envelopes can also be made see-through using special sprays. A useful way around some this of this is to use birthday cards and the like to enclose the actual message.

However, there is generally little way of knowing of whether it has been intercepted or not, so don't put anything in letters that either incriminates yourself or others.

An old trick (though less common now) by security services was to write letters pretending to be someone else in the group, or another group, to sowed seeds of dissent, so be aware of such tactics. If the language in an email or letter is not characteristic of the author, question if it is genuine. If in doubt, ring up the sender and ask them did they write it. (Though be aware that some people do have genuine issues, and it does not mean they are being deliberately disruptive.)

When posting stuff, most of what was written in previous sections applies. Anything sensitive should be done well away from your area. To write letters securely and anonymously see the separate article at the end.

6.2.5 Being aware of intruders

The State can get into any house if they want to, so they are fundamentally insecure. Of course, if you are doing nothing in your house, then this is not a problem. It is an uncomfortable feeling but one activists need to learn to live with in order to achieve their goals.

There are few locks, if any, available to the average activist, which cannot be bypassed. However, if your lock suddenly gets stiff or develops dodgy mechanism it could be the sign of a ham-fisted lock-picking attempt. Check for new scratch marks around the edge of the lock but ensure that they are genuinely new and not that you've never looked closely at it before. It could also be a simple failure of the lock, so look for other evidence to back up your hypothesis before drawing any conclusions.

Keep your house clean. It is much easier to sense if you've had an intruder if it is, as you will be more in tune with the little things that have been moved. It is a psychological thing.

On windows and at other strategic points leave a layer of dust. Thus if they've been disturbed, it will leave trails, or else be wiped clean if they noticed it.

The problem with leaving markers which may be disturbed is that by entering the room/opening the door, you may be disturbing them as well, so it is impossible to tell whether it is you who has upset the marker or not. A trick some suggest is to stand a cigarette on its filter and light it so it burns into a column of ash. Anyone walking by will disturb it, and it is impossible to replace (unless they clear up the mess and start again). The cigarette also has to be placed somewhere not completely obvious and also in a position where you entering is not going to disturb it. If using these sorts of techniques do test runs to ensure they work properly and do not give false positives.

Hair stuck on with spit is not particularly effective, as the hair can fall off as the spit dries out and your movements disturb the air in the room.

Alarms are a more expensive solution, but again not foolproof. They will stop the basic attempts, but against more sophisticated attempts they will fail, especially if you do not know what you are doing when it comes to setting them up. If you are expecting intruders, then it is best not to have stuff of use for them to find in the house or office in the first place. Certainly do not leave sensitive material lying around.

Tip: possible hiding places are in bags or jars of food, but will not fool everyone.

6.2.6 Being bugged

Police (and private investigators), either through covert intrusion or during a raid can put bugs in your house. This is why you should never say anything there you would feel unhappy about defending in court, that would give away plans for actions, or would implicate yourself and others. Or indeed gossip that could be used against you.

Bugs come in a variety of different forms and sizes and can be highly sophisticated. Most are now voice activated and designed to blend in well. Old tricks such as running water and having loud music on in the background will not necessarily be effective against them. As well as breaking in, other ways of getting bugs into your house (or office) is through 'guests', new appliances which have been intercepted, and gifts. Some offices have a policy of meeting people away from the office which will deter all but the most determined attempt to bug you (who will simply break in). Recently it has been seen that the police in the UK used wires to drop bugs into the house through eaves, so avoiding them having to actually enter the house.

Long term bugs can be hidden inside telephones and electrical sockets where they can tap into the mains for as long as needed. Others are battery operated, and have a limited life span. They can be hidden anywhere – cupboards, bed headboards (pillow talk is not safe…), sofas and in numerous other places, including clothes. They can also be embedded in objects such as cups, lamps and such like. An old favourite was in the tops of doors.

Recovering the data is the main issue with bugs, that is, how do the police get the information back? Some store information and need to be collected at a later date. Others will transmit it to a nearby receiver. The former are harder to detect and tend only to be found during renovations. The latter are easier, as they use radio signals to broadcast the information, and thus can be picked up by scanners.

A search checklist

• Open wiring points and check for devices being attached. • Lift up carpets or probe their surfaces for bumps and wires. A common place is the edge of carpets at walls as they are out of sight and easy to put in. • All air / ventilation ducts. • Ceiling panelling • Window frame mouldings for removal, pinholes or wires.	• Look for pinholes made in walls, etc. • Check the tops of doors, their frames and even inside door knobs. • Behind pictures • Drawers including their frames and undersides. • Under tables, chairs & shelves. • Devices attached to lines outside of the house.	• Use UV to detect if there is any changes in the paint. • Check the back of furniture, including looking for places where it might have been cut. • Stereos, TV's and other appliances. • Mattresses and pillows • Curtains, especially those with lining. • Vases, plant pots, books.

6.2.6.1 Scanners

Scanners are simple devices that pick up on radio frequency transmissions; they can be bought in shops (e.g. Maplins) or over the internet and are not illegal to have. Follow the instructions on using them correctly. Normal practise is to go over the house with the scanner about six inches from the wall, while talking constantly. Many bugs are voice activated so as to conserve power so unless there is something to activate them, it may not be transmitting at the time you are scanning.

There is a major problem with scanners in that they will always be one step behind the bugs themselves. When bug detectors started being able to detect transmission frequencies of 2GHz, bug manufacturers simply upped the transmission frequency to 3GHz. The real high-tech scanners cost in the tens of thousands of pounds and require professionals to operate. However, police and other investigator may rely on older equipment depending on their own budget constraints.

On one hand, many people still use bugs that can be found by over-the-counter detectors so they can be found. On the other hand it can lead to a false sense of security, and removing bugs can encourage the surveillance people to use more effective techniques. If one does find bugs your other security processes should protect you sufficiently anyway.

On a personal note, being bugged is disconcerting. It does feel like an invasion of privacy. However, if you are mentally prepared for it to happen and are taking sensible precautions then it is really of little concern that they are listening in – for what they

actually hearing? A way of turning it around is to consider it as a 'fuck-you' back to them. We often leave them in place and simply get on with our lives and taking action.

6.2.6.2 Your Car, the Garden & the Environs

Many people will assiduously check their house for bugs, but then forget to do the car, garage, garden and even local environs where it is obviously ideal for meetings such as local wooded areas and parks. All these have been known to be bugged so it is worth checking them – especially the car and garden. Similarly phone boxes in your immediate vicinity.

With the car, good places to look are:

- *Inside:* roof insulating, glove compartment, under seats and down the back of them, head rests, under the dashboard.
- *Outside*: bumpers, wheel wells, underneath, exhaust pipes, engine and boot. In more obvious places then it maybe the device is smeared with grease and dirt to disguise it. However, several have been identified by mechanics simply coming across them as being simply out of place.

Other devices used on cars are infra-red reflective tape and chemicals, both which enhances some surveillance cameras and help identify the vehicle. The chemicals can be removed by washing. The tape is white or transparent, but is often on the back, near the top.

6.2.6.3 High Tech Surveillance Equipment

Even if you are sure that you are not being bugged, your opponents can still listen in on you. For example, if they find out you are having a meeting around at your house they can simply park up and put a long ranged directional microphone in its direction, which can pick up on conversations through walls.

Mention is often made of lasers being bounced of windows to listen to conversations and read the contents of computer screens. We have not actually encountered anyone who has experienced this, though we have heard that the quality is often pretty poor, especially with closed curtains and the computer facing away from any windows. Also, if you are taking the right security precautions, you will not be saying anything in your house which would compromise you in places like your house.

6.3 Your area and neighbours

It is good to know your neighbours, in terms of whom they are and where they live. Be friendly with them, even if it goes against the grain. You don't have to tell them you are politically active, though in some cases it can actually be an advantage. Neighbours have been known to successfully rally around activists who have got into trouble.

Neighbours (and likewise work colleagues) can be a source of information both for you and the police. In the past the police have been known to approach neighbours, in particular the 'curtain-twitchers', and pump them for information on you and your activities. Some go further and will provide the police with detailed monitoring of you or even allow them to place cameras in their houses. The police may tell the neighbours outrageous lies about you in order to convince them to co-operate.

If you are friendly with neighbours, then you can pick up on people approaching them to ask questions about you, and they are less likely to cooperative with or believe your enemies. If they do believe them, you can pick up on those who have been approached by the change in their attitude.

In one case an activist found out that there was a camera in the flat opposite them because the landlord of the block of flats was unable to keep the secret and it found its way into friendly ears. Another discovered the video trained on their door when a neighbour tuning their TV picked up the images of the front door.

It is good to know your immediate area well. Draw up a map of the windows around you and keep an eye on them. Put faces to houses and windows. Watch out for windows that never have lights on, or curtains that never shut fully but where there are people entering and leaving the dwelling. It is not a definite sign of being watched but something to be aware of.

Knowing the faces is also good, as if they turn up at an action or where they shouldn't be you will be able to recognise the fact straight away. This is not common, but has occasionally happened.

As with being bugged, being watched need not be that much of a threat if you are taking the right security precautions anyway. At the end of the day, those watching you have to get results and have finite resources. If they can't get results from bugging and monitoring your home then they will not keep it up forever, or cut back on the time and effort spent on it.

One final tip for your neighbourhood is to get to know your estate quite well. Watch out for cars being parked up in unusual places, or at junctions at the end of your road where they can watch which direction you are coming out of your house. Often these cars will be non-descript, but other than the person sitting in them for prolonged lengths of time, things to watch out for are lack of dealer tags, new tyres and extra aerials. Even if people are sitting in cars with their backs to you, they can still be using

the rear view mirror to watch. Likewise work vehicles are not hard to set up so are also useful for surveillance – keep a close eye on what they are up to and which houses they are entering.

What has been found useful by some is when checking if they have a potential tail, whether at home or at a meeting, is for one person to do a quick walk, using the excuse of taking out a dog or going to the shop, to spot if anyone is sitting around in a likely car. This should be followed up between 15 to 30 minutes later to see if they are still there. This is not proof in itself, but it is worth noting the cars make, colour and number plates so that if it appears later it can be immediately clocked as a tail. If you strongly suspect a van or car is being used for surveillance on you, stop to tie your shoelace next to it and have a good look at it:

- Are the tyres too good for the model?
- Is there a collection of maps in it?
- Has the details of the garage it was purchased from on the back windscreen been taken off? Similarly, no details on the license-plate.
- Are their extra aerials attached?
- Does the vehicle or its occupants turn up in other places you frequent?
- If the vehicle says it is part of a company, ring the company to check that it is genuine (you can use a storyline such as it is blocking your drive and you want to contact the driver).

Again one of these by their own is not evidence, but they all play into the pattern you are watching out for. However, sometimes you will get clear markings that it is a state-owned vehicle such as saying 'Police' on the tax-disc.

6.4 Your Vehicle

Your car is a very useful way of tracing back to you, and building up a picture of your activity, especially if the car is used for group activity. A useful technique for minimising this is to regularly change ownership of the vehicle. Generally you can do this as often as you want. In the UK a vehicle can only be registered to a PO Box if it is in the name of a registered business.

The State, as a rule, is very keen on who drivers of vehicles are, as to their way of thinking it is a position indicative of a leadership role, and also useful people to take out in order to cripple a group.

6.5 Self Defence

Security also includes protecting yourself from physical harm. When out and about being active you never know what sort of nutter is going to attack you, and that includes enraged security guards, hunters, etc. Learning a few basic moves on how to break out of grips and disable attackers long enough for you to get away is important.

Many self-defence courses will teach you what you need to know.

6.6 Your Personal Profile

A large amount of police work and surveillance s focused on building up personal profiles of individuals. This allows them to be placed in their network of hierarchies which are assumed on how groups work, and also to categorise people, whether as a serious treat, someone who is only an incidental player and so on.

An important part of this is building up a picture of your contacts, even if you are not discussing stuff openly. This is why they are interested in who you are talking to on demonstrations, or who is visiting your house. Even if they are not getting information that will convict you, it is still being absorbed.

As a part of this, the state and corporation are keen on finding out who are the signatories of bank accounts, whose houses the meetings are in, who the drivers are, as these are the people they equate with being the main organisers and thus to get the majority of the surveillance effort.

Corporations are also interested in this sort of information as it allows them to go to court to get injunctions against people, and to tie people in together. Even if the evidence by itself does not amount to much, it can all be thrown into the mix. Saying this, if you are completely open in your activism, or your cover has well and truly been blown, then much of this is not a matter for you personally. By taking other security measures you can continue being a campaigner safely, and even covertly. Where it does come problematic is that having become a point of focus it can be a tool to lead the powers that be to others who might not have risen so high on their radar.

There is no privacy in prison; if you write a letter to a prisoner, or even visit, the chances are that it will be logged, especially where there is a political aspect to the case. In the UK phonecalls made by prisoners can be tapped and used in court cases and have been, without any of the other safeguards currently in place. The obvious tips are to
a) use a different name if writing;
b) preferably type rather than handwriting, even if you are using your home address, and
c) if a prisoner, avoid saying people's names on the phone.

The aim is that even if you are in communication with a prisoner, then it is harder for the state to use that evidence in court, even if they still assume for their own profiling that it is you who is involved. If this sounds a bit paranoid, in one campaign the evidence connecting one individual to it is based on a prisoner greeting her by name when the prisoner made a phonecall to the campaign office.

6.6.1 Your Online Profile

Online networking sites such as Facebook, MySpace, etc only help them in this. People give away huge amounts of personal data and provide clear details of who knows who, and how well. As an interesting exercise pick a random profile and see how much you can learn about that individual; by combing their friend's websites you can also find out further details of what they have been up to, their politics and so on. Also consider what would happen if your online profile was pulled out in a court case. What sort of trouble could that cause to any defence you have, for example, what groups would it show you supported. A related issue is that others also use popular networking sites to monitor existing and potential employees so you may need to engage in some self-censorship as to which groups you support, especially if they are been leaned upon to fire you.

If you are on a site like MySpace, avoid putting up personal photos of yourself or giving personal details such as your date of birth, and so on, again something which helps identify you. Or else give a fake one. If friends have put up photos of you, ask them not to "tag" you with your name or common identifier so others combing their sites for details about you will not be able to immediately grab an image of who you are.

It is not only networking sites to be cautious on – any sort of bulletin/messaging board retains you posts for everyone to see, and many will also log your IP address. Email lists can be published easily enough on websites or joined by people you do not know. There is nothing stopping you using email addresses or online identifies that do not relate directly to who you are – chose random monikers (not your hamster's name) for your email address or identity; if personal details are not important for the site, eg. date of birth, home town, then do not enter them in.

You may also want to consider what you buy online and how that will tie in to your profile or could be used against you. Consider getting a friend to use their credit card to buy your travel tickets, etc.

Another problem with the online world is how much information is retained by companies such as Google, Yahoo, etc. Search engines can create a history of your online activities dating back over a decade, and are a gold mine for those investigating. It builds up a good idea of what you have been doing, where you have come from, various scraps of personal details which can all be added together and so on. This is something to be aware of both now and for the future, as once you are there, it is incredibly hard, if not impossible to have information removed.

Again, all this depends on your actual security needs. How much information you give away is up to you, just be aware of how it might help others who would be interested in finding out about you for reasons not so benign.

7. Surveillance

Being put under surveillance is a fact of life for the political activist. It is actually a sign that you are being taken seriously so it is not always something to be concerned about. It is certainly not being paranoid to think it could never happen. It does, and much more regularly than is supposed, though not often in a systematic manner. There is no basic right that stops you from being put under surveillance, so relying on the law or the fact "you are not doing anything wrong" are no protections.

In the following we deal with how to detect and evade surveillance when you are on foot or in a vehicle, known as "physical surveillance". We will not go into technical approaches here, though they are often an integral part of a surveillance operation as well.

There are several different reasons to be followed. The main two are intelligence gathering and to intimidate. The latter is dealt with at the end. The third category is because you are suspected to be involved in criminal behaviour and the police or intelligence services anticipate stopping an action. Depending on which situation you consider yourself to be in, then that should feed in to how you react.

All activists, and even individuals only connected on the periphery of a group or campaign, will be watched at some stage, including active surveillance of their lives. The main purpose in doing this is to build up a profile on people so there is at least a basic file on you (e.g.. name and up-to-date address to go with a photograph) and so they have a good idea how you fit into the organisation or group they are targeting. And also whether you are worth a closer look (a reason would be hanging out with other activists who are known to be involved in covert actions or organising). High profile activists, especially outspoken ones, will be under regular surveillance as a matter of routine. Most others will have periodic surveillance as the State seek to update their intelligence and profiles. The mistake is to think that surveillance only happens prior to actions or arrests.

Of the people who are likely to follow you, there are two approximate categories:

a) The professional with money and resources behind them. These can be either private investigator working for a very big corporation, or skilled State operatives from the intelligence services.
b) Everyone else, which includes your standard private investigators or police officer who has had minimal training with limited resources and time.

The latter is generally easy to spot once you are looking out for them. Tailing someone is much harder than you would expect, especially if the person being tailed is taking measures to spot or lose any surveillance. Many police now simply follow openly as they are too visible to get away with it, and their aim is often to deter rather than arrest.

If you are the target of a major operation then they will throw far more resources your way which makes detection far more difficult. For instance, it is rare for just one car to be used. In one operation 14 different vehicles were involved in follow an activist's car along a motorway. For the professional, surveillance is just as much about not being detected as it is following the target. Being followed by professionals is very hard to detect. It can be done, but it does require effort and planning to be successful. Professional surveillance teams are ready for counter-measures so if you are in a situation where loosing them is important then it is not going to be a trivial exercise. The problem is that as you lose one tail, another coming from a different direction can pick up where the first one left off – even easier where you are following an established pattern.

However, our experience of surveillance on activists indicates that those doing the tailing have fewer resources available than is ideal so can be spotted with many of the techniques we discuss below.

The main question the activist needs to ask themselves is how they want to deal with surveillance. This may have significant consequence both for the reaction of the surveillance team and the campaigner's actions. If you are not particularly engaged at the moment in activities you would rather the state did not know about, or they are simply doing routine surveillance to update their files, then we suggest, as a rule of thumb, that you do not let them know that you are aware. Instead, avoid drawing further attention on yourself and focus on confirming whether you are actually under surveillance or not. Save active anti-surveillance activities for those moments when you need to confirm that you are indeed not being followed before potentially compromising yourself or an action.

If you are dealing with relatively amateurish tails it can be quite empowering and fun to run rings around them to the point that they give up.

This depends on what you are doing and what sort of campaigning you are engaged in. If you are the sort of activists who is well known to the State this is more appropriate behaviour to engage in, than someone wanting to keep a relatively low profile. Often, surveillance from demonstrations is for intelligence gathering purposes; that is, to identify people on the action and where they live for future surveillance. In this case, losing the tail makes their job much harder – why give them intelligence on your group on a plate?

In some cases police openly follow activists to disrupt an event so losing them becomes useful; some of the techniques we discuss below on an anti-surveillance are also applicable to dealing with this sort of problem (though it is also useful to be a decoy if you have the appropriate profile).

One advantage of confirming a tail is when you force a tail to expose themselves or making them realised they've been spotted (known as “burning”), then you destroy their usefulness as a tail so taking them out of the picture and stretching the limited resources devoted to you even further. Undercover police will get quite freaked out at attempts to photograph them, as when their pictures are published it destroys their ability to continue as an undercover operative. Though be careful as the police have been known to raid houses/offices and seize equipment solely for because of this, so take care.

Using anti-surveillance techniques on a non-professional tail can encourage them to learn from their mistakes and become more cautious in future. They will be better prepared to handle other counter-measures you use in the future as well. Thus, if you are planning to burn a tail then it is best to do it properly to make sure they do not come back. This is always a problem with anti-surveillance. It also encourages the more amateurish surveillance to brush up their techniques so it is harder to spot them in the future, and it brings attention to yourself so encourages the use of more sophisticate methods.

Like most things relating to security, awareness of surveillance should be part of daily life for a political activist. Developing your skills and instinct is very important here. You can develop your observational skills without being under actual surveillance or without having to act evasively. With personal security, your instinct can help you detect if there is something out of place in your environs which you need to pay closer attention to, the same goes when you are moving around. What starts as something unnatural and awkward at start eventually becomes second nature and you barely notice the fact that you are scanning an area for vehicles and people who are out of place. It also means you appear more natural when doing it, and less shifty.

Also, like other matters in security, it is not the sort of thing that you can stop and start with at whim. By the time you have noticed surveillance, the chances are that if they are at least semi-professional about their job, they have probably already been at it for several days and you are behind in the stakes. It will not be hard for them to move up to more sophisticated methods while you are still trying to identify the surveillance team. Surveillance will take place over many days so it is useful keep what you’ve noticed in mind (or make a note to remind you) in case the same face or vehicle does appear again at a later stage.

Similarly, you need to beware of being unnecessarily paranoid when it comes to detecting surveillance. A suspicion that you have seen a face or car before is not evidence enough that you are under surveillance. To be sure you have to wait until evidence builds up until it is conclusive. This requires that the activists is being constantly observant and being pro-active in singling out faces and vehicles to pay closer attention to. Or that you take active anti-surveillance measures to force their hand.

Another situation to be aware of is where you are preparing for an action. Suddenly looking over your shoulder and acting erratically may give them the impression that you are up to something so deserve further attention. This is why surveillance detection techniques should be employed regularly so even if they are monitoring you they will see it as being part of your life, and not sudden changes. Plus the more you practice the more discrete you are able to make it, and the more you develop that all important instinct.

When you do undertake anti-surveillance techniques, have it planned out in advance. Make sure it is thought through, and you know what exactly it is you are looking for - “anything suspicious” is not good enough. Furthermore, have it ready so that they are not expecting you to take that sort of action. For example, travelling down an obscure road the night before an action is too late as if they are watching you then you are just giving them time to prepare for when you do it again. Such anti-surveillance routes should be planned well in advance, and created as what appears to be part of otherwise natural behaviour (e.g. visiting a friend or going for a hike), and it is best to have several ready.

Our final point is that surveillance is also static. Houses nearby you can have people who will let cameras and men be established in their front rooms so they can monitor your coming and going. If there is an empty flat, it may well have a motion -sensitive camera taking a photo of everyone entering or leaving your house. This has been known to happen. Stationary vehicles are also used, though more obvious.

Given the variation in experience of surveillance teams and of local geography, there are no absolute rules when it comes to dealing with the issue. Everything offered is guidelines and there will be times when they do not apply or you need to think in different ways. Thus the following sections are divided primarily into vehicle, foot and static surveillance. These are further divided in to urban and rural situations. Sub-headings in these are passive, active and anti-surveillance techniques, that is in each given situation we start with passive observation techniques, move on to more active approaches for confirming that you have correctly picked up your tail, then tactics on how to lose them if you so wish. To make it easier, we suggest that you first familiarise yourself with the following glossary.

Glossary

Target: the person or vehicle under surveillance. Also referred to as the *Principal*.

Surveillance Team: the group of people carrying out the surveillance on the target.

Command: the member of the surveillance team who has the target in sight and is doing the active tailing.

Stakeout box: where a stationary target is surrounded by the surveillance team to be ready for when they move off or to monitor their activities.

Trigger: member of surveillance watching house or stationary target, waiting for them to move. They initiate the actual tailing though they do not necessarily do tailing themselves.

Pick-up: the point at which a surveillance team member or vehicle beings to follow the target, normally becoming the command at that point.

Counter-Surveillance: the use of a second team to locate and identify those putting the target under surveillance.

Anti-Surveillance: taking action to lose a surveillance team.

Passive: measures used to identify surveillance without changing your routine or patterns; avoids alerting surveillance team.

Active: taking measures that will allow you to identify surveillance that involves the target taking evasive measures. Can be overt or covert depending on whether the target wants to avoid alerting the surveillance team or not.

Target Pattern Analysis: a study of the target identifying their habits and other routines, allowing for easier surveillance.

Expose: if a surveillance team member or vehicle is visible to the target, then it is said to be exposed. The target may not be aware of their presence.

Burn: a surveillance team member or vehicle that has been positively identified as a tail by the target is said to be *burnt*.

7.1 Preparation for detecting surveillance

The core of surveillance is target pattern analysis. That is, the routine and habits of the target, the person being followed. This covers many things, but in particular stuff such as: what are the regular routes taken to and from places, driving style, who they visit and so on. What they are seeking to do is to be able to predict your movements to make themselves less noticeable and the surveillance job as a whole easier and less resource consuming. Do not assume that because stuff feels obvious to you, such as how you get to and fro from work and where you work that its is to them. They still need to confirm it.

Target pattern analysis is of singular importance as it is at the heart of more sophisticated surveillance planning. Target pattern analysis means that as you drive off, it is not the member of the surveillance team watching your front door that follows you, but the vehicle waiting out of sight a few hundred meters away along the route you normally take. It is often the moment you think you have got away that you actually get picked up.

Many of the techniques that are used to recognise and deal with surveillance are based on the target being aware of what sort of information any surveillance will have picked up on them. In other words, you work out what they will have learned about you, and you use the fact they are depending on it to defeat them when it comes necessary. Just as they analyse you, you analyse them. Knowing the standard procedures used for surveillance makes your own analysis of what they are looking for in your daily routine much easier. Knowing what to watch out for make detecting surveillance a lot more meaningful and easy as well.

This also means that you need to know your area well and identify observation points that could be used for watching your house and vehicle. Where would the trigger be, and were would the pick up be potentially situated? Mark them on maps of the area, including which direction any vehicles are likely to be parked in. If you know which points to keep an eye out at then picking up suspect tails becomes much easier and second nature.

If you think that you have been under surveillance for a period of time already, you need to consider what patterns of yours they have already picked up and could be using in their surveillance on you.

How you plan your surveillance detections depends greatly on what your intention is. You need to decide if you are going to let on or not; whether you are planning to lose them or do you not really care at this stage. Sometimes this will depend on the day. For example, if you are part of a large public event they may start attempting covert surveillance on you hoping that you will lead them to anything planned they may not know about; however, if it becomes clear that you have made them then they are likely to switch objectives to simply keeping tabs on you with the command operative that you have identified. This is to disrupt your activity, as they may assume that you are some sort of crucial organiser.

Draw a map of the buildings around you. Which windows always have blinds drawn and show no sign of activity or lights ever being turned on? Who are the regular visitors to your street and what is their typical appearance? Likewise with vehicles.

Every area will have pros and cons when it comes to surveillance, hence why it is as much an art as a science, and there are only guidelines. However, knowing what to expect and planning out surveillance detection measures will turn your observations from guesswork and paranoia to proper confirmation of whether surveillance is actually taking place or not.

7.1.1 Surveillance team techniques

Before you get ready to spot for surveillance it is worth knowing the typical behaviour of a professional surveillance team in action. Understanding how they work makes it easier to watch out for the giveaway behaviour and take appropriate actions to detect or evade.

Trigger

The trigger is the person or vehicle who is watching out for the target to start moving. They can be parked up in vehicles on foot. It is rare that they start following once the target has been spotted, but instead tend to move in a different direction once they have confirmed the target has been sighted and what direction the are moving in.

In less experienced teams, they can get into the car that begins tailing – a dead give-away.

The Command

The command is the person or vehicle which is currently tasked with keeping the target in sight. Their behaviour as they attempt to do this is what you need to be looking out for.

Where there is a team of experienced surveillance operatives, then the command will change regularly to avoid giving themselves away. If the command feels that they have been exposed to the target too long or that they have noticed him, then they will be changed at the next opportunity.

In amateur surveillance or where there are limited resources, then the command often remains unchanged or reappears again.
In sophisticated surveillance there will be a number of vehicles or foot operatives located nearby who will be in communication with the command. The preferred technique is to traveling parallel to the target and the command. Thus when the target makes a turn, the command simply continues traveling on straight, allaying suspicion against them. They cease to be command and take up position as one of the flanking operatives. Meanwhile, one of the parallel members of the team on the side which the target has turned will take up position behind them as command, with the target thinking that the vehicle has turned up behind them by accident.

This technique works best in well laid out cities and towns. In places where there are bendy roads, on motorways and on rural roads it becomes much more difficult; thus the opportunities for detecting and evading surveillance increases greatly.

Observation Points

An observation point is used to keep a place under surveillance. It is placed within sight of the place but preferably around a corner or where there is good visibility of possible routes that can be taken. When out and about the observation is often a side road that gives line of site and the ability to change direction as needed.

Can be a house, but is more generally a vehicle. If it is a vehicle then is likely to be a van, camper, etc where the interior can be hidden. Points to look out on them are extra antennae, not seeming to belong to any building in the area, curtains and other material that stop the back being seen into.

To allay suspicion it will have a separate driver who doesn't remain with the surveillance team, but comes and goes as they need him. Such drivers will have another vehicle stationed nearby, or arrange to be picked up by another member of the team.

Where the observation point is in a house, watch for windows which are kept covered and devoid of activity, e.g. lights never turned on. There may be unusual visitors to the building, generally on foot as they will leave cars out of sight in case the are made by the target. Shift changes will often happen late at night so they are not noticed, and with modern equipment they do not even need to have people present. Keeping a map of the surrounding buildings and all their windows allows you to monitor activity where a camera may be placed. It will have good visibility of your doorway. Empty flats are also known to be used. A good network among neighbours has been quite good at routing these out.

In once case, a camera was placed facing an activist's door and transmitted to a recording device some distance away. This was detected by a neighbour tuning their TV and picking up the image of the door. The camera was identified and from there the recording device was also found.

Stakeout Box

Any time a target stops the surveillance team set up what is known as a stakeout box around them. The purpose of this is that they are prepared for whatever direction the target decides to move of in next.

It makes spotting the command vehicle difficult at this is often the point at which they change. However, the stakeout box is a pattern, whereby the surveillance team takes up points that give advantages in following you. They will use side streets and park in the direction of the flow of traffic that they expect you to take. Often they will park in directions point away from you as that will be the way you will be traveling should you take that route. Thus when you set off again, the command will come out of side streets behind you. However, if you are aware of your surroundings and can identify where they are likely to be parked, then this can be detected.

If the stakeout box is around regular places such as your house, etc, then they will use target pattern analysis to decide in advance the most likely routes you will take. This means they can park further away. It is worth taking walks to shops or nearby friends, or even dog walks, that will take you passed such point you have identified so you can observe them covertly. This is a good technique to build into your everyday life to check if you are being watched.

On foot the situation is more difficult for them, but if you going in to a shopping centre then they will try and cover all exits.

Lost command routine

When a surveillance team loses sight of their target they will attempt to find you as opposed to give up. The first thing they do is search down the surrounding side roads or alleyways to see if you have turned down any. If they fail to find you there, they will return to where they lost you and continue in the same direction as you were last known to be traveling, with speed. This is why returning to the area where they lost you is a bad idea, as is parking up nearby once you have given them the slip, unless your place of concealment is quite good. While you might know one or two of the vehicles following you, you may not have spotted them all and you could simply be picking up another one of the team.

If evasion is not you goal, then you can use this routine to burn operatives, as it is difficult to relocate you and avoid detection at the same time. For example, parking up and wait for them to come searching. In one case the suspect vehicle drove by and was clocked by the waiting activists; it went on to park up around a corner, aware that it cover was potentially blown. The activists then drove up next to it and engaged them in conversation, making sure everyone had a good look at the surveillance team's faces. They looked very uncomfortable. If evasion is not an issue then it does not matter that if they are police then they will give up attempting to be covert, and simply follow you overtly.

Exposure

Surveillance operatives are desperate to avoid exposure, but it takes a particularly skilled operative to avoid betraying themselves when they are caught of guard. If there is a team working on you they will have only one operative or vehicle exposed to you at any one time (including trigger).

Avoiding eye-contact is the usual one, and operatives may go out of their way to avoid it, even tripping up in their efforts, depending on how skilled and prepared they are. Less skilled operatives will show their surprise and anger. However, much body language is instinctive and they may not realise they are giving out signals tipping you off.

It is also worth allowing patterns to be established as this lulls them in to complacency and dropping their guard slightly – surveillance is hard to keep up for a prolonged time at the same level of intensity. Thus, when you break the pattern, they are more likely to show their surprise. When you are traveling a route not normally taken, or is new to you, then they are automatically more alert to your actions.

7.1.2 What to watch out for

Vehicles

When you pass suspect vehicles, the driver and passengers may go out of their way to not glance in your direction, looking away as they pass you or staring ahead fixedly. Watch how people react normally and then compare it with those you suspect.

Can you see them repeatedly pressing buttons on a radio as they talk? Are they talking repeatedly and peering forward?

While on foot when a suspect vehicle passes you does it speed up as it passes; does it quickly turn down a side street?

On foot

It is much easier to spot giveaway body language when being surveilled on foot. Look out for:

- Coughing, tripping and other behaviours of someone who is being distracted when there is no obvious reason.
- Signs of tensions such as pacing, focused staring, checking the time repeatedly, twitching.
- General awkward mannerisms.

- Speaking into collars or their chin lowered into their chests as they speak.
- Touching their ears repeatedly is instinctive reaction to an ear-piece in use.
    - Is there a wire running down to their collar? Though with the prevalence of personal stereos and mp3 player this is far more common place and harder to detect unless it really looks out of place with the rest of the person's attire.
    - Do they stop and stare into nothing – a feature of someone taking a message.
- Adjusting clothes hiding communication devices or repeatedly putting their hands in their pockets to manipulate a communications or listening device.
- Clothes out of place for the venue (e.g. suit in a punk venue, etc).
- Startled look as they encounter you unexpectedly in active detection techniques
- Bad window-shopping (compare how people usually do it by moving their heads, as opposed to a tail who is trying to see in the reflection or not properly looking at all).
- The same person taking yet another phone-call.
- Someone in a phone-booth doing more observing than actual talking.
- Avoiding making eye-contact at all cost.
- General uncertainty if you break an established pattern.
- Are they carrying a bag with a video camera in it?
- Carrying out repeated scratching of head or checking of watch – possible non-verbal communication signals.

Appearance

A surveillance team will attempt to blend in. They will not be dressed in sharp suits and sunglasses and look like something out of Hollywood. They will use operatives who are non-descript and who do not draw attention to themselves by having features that stand out. Often they will be the same sex as the target as this helps allay suspicion and attention. The key to successful detection is to put preconceptions aside and watch for people's behaviour and not their appearance. Appearances including clothes can easily be changed by someone who knows what they are doing.

Saying that, the amateur is not able to indulge in the techniques of a professional and as a result much more easily picked up. Also, if the territory is unfamiliar then they may get the dress code wrong and generally show signs of discomfort.

Night observation

At night the world is a different place; you need to be more in-tune with how noise and silhouettes change in the dark. Likewise it is worth developing you night vision: this takes about 30 minutes and you need to avoid bright lights or you will ruin it. When looking at things use off-centre viewing or scan rather than looking directly.

Remembering details

Vehicles

Tips to help with this are to look for

a. Body shape
b. Shape of headlights
c. Dents or scratches or other distinguishing features such as broken lights
d. Silhouette at night.

Individuals

With individuals you need to focus more on the general appearance, demeanour and the mannerisms rather than on small details. Tips to look out for are

a. Facial hair
b. Hair colour
c. Unusual features such as scars
d. The shape of the face

Remember some of this can be changed by the use of wigs or simply changing clothes (dark to light, etc). Body shape can be hidden by wearing baggy clothes.

7.2 Vehicles

If you think you are being tailed use routes and techniques that will make it obvious. The following are some techniques to identify and deal with surveillance. The sort of vehicles can be any type but they will on the whole be non-descript and of generally common models and colours. There will be nothing fancy. There may be some modifications that give them away such as tires too new, the car being too expensive for the area where it is stationed, markings of where it came from removed and signs of prolonged occupations such a coffee cups, fast food containers and scattered maps.

7.2.1 Urban

Passive detection

a. When going to and from your car use the opportunity to look at the surrounding area for people or vehicles that might be acting as triggers for the surveillance. Depending on the area the trigger may be on foot as opposed to in a vehicle. Try not to stop and stare but make it natural. If you've already worked out where in particular you should look it becomes quite easy.

b. Are there vehicles near your home, work or places you frequent regularly which have people sitting in them? Often they will have their sun-visors down permanently; this is done to stop faces being fully visible. This is surveillance that is poorly resourced or where they want you to know they are watching you.

c. Number plates:
   d. Memorize number plates: if you spot a car you are suspicious of, look at the number plate and turn the last three letters into a word, e.g. BCH becomes BaCkHand. Words are easier to recall than numbers and letters, and if you come up with the same word again you can pick up on it quicker.

   e. Watch for number plates that do not have a garage name on them; police tails are often missing these. Note, this is not a guarantee the vehicle is definitely a tail. Some unmarked police cars actually have police written on their tax discs.

f. Does the vehicle look out of place for the area you are in? It is harder to identify when out and about unless you know the area quite well. Or does the vehicle look modified. See the section on personal security for more on what to look in a vehicle parked up like this.

g. As you pass identified pick-up points, watch the parked vehicles. Often they will park in the same direction as you normally take and on the same side as the flow of the traffic.

   - Can you see maps and signs of people sitting in them for a while, e.g. coffee cups, food packets on the seats?
   - If possible check the exhaust to see if it is running and waiting to go.
   - In cold weather are they getting out to clean the windows regularly?
   - Do they pull out behind you as you pass?

h. Vehicles tailing will generally drive two to four cars back. Depending on the nature of the traffic and the road, they need to keep you in sight, so watch out for vehicles pulling out of the line of traffic (both sides) and then drifting back in. There will be points at which they close up on you, depending on obstacles and other traffic situations, e.g., road works, traffic lights, heavy traffic. This gives you a chance to get a closer look at them. One bit of suspicious behaviour is where a vehicle slows down prematurely so as to avoid coming right up behind you, so upsetting the flow of the traffic. Surveillance drivers often instinctively of pacing their driving to the target vehicle will disrupt the flow of traffic.

i. At junctions, traffic lights, etc, the surveillance vehicle will often get closer to the target vehicle to ensure they can see which direction it is intending to head in. However, if they feel that it has become too exposed it may turn in a different direction to be replaced by another vehicle, though this depends on the resources at hand. If you suspect a vehicle and it does turn off, still keep a note of its details in case it reappears at a later time or day.

j. On longer stretches of roads, surveillance vehicles will have a tendency to pace each other in a convoy; that is match each others speed and keep the same distance apart; they are unlikely to overtake each other. This becomes a recognizable pattern that can be spotted. They will be in front and behind the target vehicle, with ones in front allow you to over take as command is changed around to avoid the target getting suspicious.

k. They will also pace themselves to the target vehicles. This allows them to be spotted through careful observation. For instance, depending on how they change speed, they will travel fast to catch up with you. As they get close to you they will slow down and pull back instead of overtaking as you might expect. Do they drop back to the same distance they were previously?

l. Adverse weather conditions will cause surveillance vehicles to drive closer than they normally would due to poorer visibility; in particularly bad weather they will drive in front of the target vehicle.

m. Keep up observation at traffic lights and other suitable places.

n. Driving at night, the tail may wish to ensure they are following the right car, so will buzz you so they can read your number plate, then either pull back or over take (before falling back later). If you believe you are being tailed, keep an eye on cars that have buzzed you.

o. Enter a petrol station and see who else follows you in. Is there a car that is not refilling or simply parks up? Does anyone follow you to the shop but doesn't buy anything? Can also use car parks for this, but they are harder to confirm suspicions with given their general geography, though it does allow you to narrow down the set of vehicles to be considered suspect. Likewise with a lay-by on a motorway or main road.

p. If you are in a service stop or petrol station for some time then a stakeout box will be set up around it (or in it, as in the case of a service station). This provides opportunities for you to look for the tell-tale signs as you return to your car or leave the site. As you do so, take one of the nearby side routes as opposed to the main road, if there are such opportunities. This is were you are likely to encounter surveillance team vehicles waiting – they may be parked facing away from the petrol station, etc in case you did take this route, but they still have to pull out and follow you, so giving themselves away to the person who is watching for it. If you are able to observe on the way into a petrol station you may actually witness the surveillance team set up their stakeout box.

q. Stopping to eat in service stations gives you an opportunity to monitor faces and vehicles coming in. If you are placed at a window you may spot them checking your car for phone-numbers/maps/papers with directions as to where you are heading.

r. In a multi-story car park who follows you all the way up to the top floor to park?

s. Pull of the road and lift the bonnet to your engine as if there is a fault. Does anyone pull up in front or behind you, or stare at you as they go past?

Active detection

Erratic and sudden changes in driving are among the most useful techniques for detecting surveillance. The idea is that you force a reaction from them. In order to keep you under surveillance they will have to expose themselves with unnatural manoeuvres to match yours, or demonstrate uncertainty. The more professional a team is then harder it becomes as they will have the training and resources to not give themselves and to pick you up with another member or vehicle. You are also letting the surveillance team in on the fact you suspect you are being followed. Many of these techniques described here are equally applied to anti-surveillance, where the aim is to loose tails. In this case the surveillance teams are seeking to avoid exposure and end up having to let you get out of sight.

a. Erratic driving includes
   a.1).running red traffic lights, or attempt to clear them just as they are turning red; often surveillance teams will not follow as it exposes them so this is also an anti-surveillance technique.
   a.2).cutting down side streets (beware of picking up surveillance vehicles moving parallel) and other short cuts;
   a.3).illegal turns.

b. When you take turns or side streets there is a possibility that you will encounter one of the other vehicles in the surveillance team, perhaps one that has previously been command and you have already been suspicious of. Thus you should look to see what other traffic is also appearing as opposed to what is behind you.

c. Pull into the side of the road at a green light; who else waits behind rather than go through?

d. If you are aware of a blind turn or a sharp hill, drive fast into it and once through it slow down immediately. What vehicles are bearing down on you as they attempt to get you back within sight? Do they decrease speed rapidly to stay behind you or do they realise they have been burned and over take to get out of the area. A variation is to pull in immediately and look for the reaction of suspect vehicles passing you.

e. Do a U-turn.
   e.1). Who attempts to follow?
   e.2). What vehicles behind you attempt to park up? Do they turn in your direction in an attempt to pick you up again?
   e.3). What is their reaction as they pass you?
   e.4). A variation is to pull in and wait for any suspect vehicles to pass you before doing the U turn.

   In light traffic these reactions will be quite obvious, and in heavy traffic they will cause more commotion in attempting to do them, both playing into your hands.

Standard practice for the professional is to continue traveling on and not to turn until the first opportunity comes along rather than doing their own U-turn. However, in our experience this is a good method for exposing the surveillance tails where there are fewer resources available to them.

f. If you are a good driver then you can combine the U-turn with the blind corner / hill crest; this combination is much better at forcing reactions as they are not prepared for you having turned around.

g. Take roundabouts several times (though under UK law three is the maximum number of times that you are allowed to this), though the successfulness of this depends on the size of the roundabout, the heaviness of the traffic and how far back the tail is.

h. Indicate to take a turning at a junction and then go straight on. Has the suspected tail done likewise? This not particularly effective as tails often don't indicate at all because of this and being several cars behind means that they can react to your change without giving themselves away. Works best for where the car you suspect is immediately behind you.

i. When parking on a street chose a direction opposite to the one you leave in. Allow enough time for a stakeout box to set up. You are looking for uncertainty in the trigger on the unexpected behaviour, or vehicles doing inappropriate U-turns either to stay in the same direction as you. It also means that more resources have to be committed to tailing you so increasing the chance of detection.

j. Cul-de-sacs are ideal for picking up on tails, and with amateur tails for losing them. However, your tails are also aware of this. Go down the cul-de-sac and wait a few minutes before leaving again. The tail will do one of two things:

   1) Follow you down the cul-de-sac (though you may need to allow them a few minutes to make this decision). In which case you can immediately spot them, especially if it is a car that has been with you for a while. Plan to turn your vehicle as soon as possible though out of site of the road you've come from. On a narrow cul-de-sac you can be gone before they have a chance to turn around.

   2) Wait on the road outside the cul-de-sac knowing that you are practicing anti-surveillance techniques. As you stop at the top of the cul-de-sac waiting to rejoin the flow of traffic, watch out for cars parked up with the entrance of the cul-de-sac in sight and who start moving once you leave the cul-de-sac. Driveways may be used as well, but may depend on high enough housing density to work.

   If the cul-de-sac is signposted and your tail is professional then they will not be caught out by this, but it still often works on the average investigator or police who have not got much experience tailing people watching out for such activity.

j. In suburban areas go for streets that are curved as opposed to a grid-like structure. When you think you have got the tail out of sight, swiftly drive down a side street and get around a corner before parking up. In this case the tail will continue to search for you and eventually come back down the side street, thus giving themselves away.

   In some cases they tail will actually stop. Further up or around the exit point is usual. As by this time it is probable that they realise they've been clocked. However, unless it is heavy-duty operation, they will quite often wait around to see what you will do anyway. In this case we suggest that if they have already been in a position to see the faces of who else was your the car, then you pull along side them to have a good look at their faces, even photograph them (you have a good excuse by saying that you thought they were trouble, though it in turn could be inviting them to harass you further, so balance out the risks), even ask them a question for directions. It allows you to find out what they look like, while at the same time letting them know their cover has been blown.

k. Use routes that are not obvious to get to your destination such as taking the long way around an estate or several blocks when there is a blatantly easier way to reach it. Works better for a destination they are not aware you might be heading to. It can be a destination you have picked solely for this purpose.

l. Having left your starting point, take a different route back to it. Does anyone follow you back, even to the end of the street?

m. Motorways and other major roads provide different opportunities for spotting the tail. As the travel on them is faster the command vehicle and their team also need to be able to react faster to keep you in sight. They may have to allow for the fact that if you come off at a junction they need to see which way you have gone. However, at night and on roads with long range visibility and low density traffic on them it may be that they do not need to be as close. Remember though, that if you force the hand of one surveillance vehicle, then it may be replaced by one traveling further behind it.

n. Who follows you into a service stop or over a junction and back onto the motorway? This is not typical behaviour, but if they want to keep you in sight they may have to commit to it, though if a professional realises what you are doing in time they will lose you but let a vehicle further back pick you up further down the road. However, you have potentially taken one vehicle out of the operation. This is not a tactic that will work with repetitive attempts as the will soon get wise to it. A more covert method, if you are not ready to let on you've identified the vehicle is at a complicated junction go around in an odd way that takes you back onto your original route, or even in the opposite direction. Which vehicles have had to get close to follow your and also taken this odd path? This may require some prior planning to be successful against an experienced team.

o. Slow down to exit onto a service road or junction, but at the last moment pull back out on to the main road – who does likewise?

p. Just before an exit from a motorway pull into the hard shoulder. Standard procedure is that the command vehicle will leave at that exit so you may be able to identify them.

q. At tolls chose the longest queue to go to. Who does likewise? Does anyone go through and pull up or drives slowly until you pass by?

r. If you are pretty confident that the vehicle right behind you is keeping you under surveillance, do an emergency stop that forces them to go into the back of you, or come very close. Get out and check their reactions – often they will simply drive off rather than engage with you. If you are a bunch of big men getting out aggressively they my drive off out of pure fear rather than because they are tailing you. If they don't it gives you a chance to confront them.

Anti-surveillance

j.1). The best way to lose a vehicle from home is to follow an established pattern to start with, then to suddenly break it by taken unexpected turns or traveling at speed down roads, thus forcing them to take a choice of either losing you to avoid exposure, or exposing themselves, so effectively taking themselves out of the surveillance team.

j.2). Both situations are opportunities to be taken to lose them, and move out of sight altogether. Techniques for doing this are extensions of the various active detection methods above, where instead of watching for reactions of possible tails you are using the opportunity to get away from them altogether.

j.3). If you are aware of a blind turn or a sharp hill top which cannot be seen over, either of which has a second turn immediately afterward, you can use this to get out of sight.

j.4). If you are using vehicles, park up where you have quick access to a foot only route taking you to another road where a colleague is waiting in another vehicle to whisk you out of the area.

j.5). If you know an area well, then consider concealment in little lanes and long driveways, though this is very much dependant on the terrain and how well you can remain concealed while they are searching for you.

j.6). Go for dense traffic, and weave in and out of it. It is much harder to follow someone in these circumstances; use routes they are not likely to have anticipated.

j.7). At night switch off lights and pull into concealed places or even driveways (unoccupied houses or pretend to be lost to the owners).

j.8). Bikes are much harder to follow than vehicles; especially in places were there are many cycle ways distinct from roads, allowing you to disappear out of sight. It is easier to loose foot surveillance, and easier to detect if anyone is attempting to follow you, as other bikes tailing you and especially cars stand out a lot more. Planning is still needed as other members of the surveillance team may be waiting at the end of the cycleway for you to reappear.

j.9). For observation vehicles, or even individuals, there are several things to do with them:

- Call the police on them with a story of why you suspect the vehicle and observe the reactions of the suspected surveillance. Often the police will not turn up, but the surveillance vehicle, knowing they are now being watched themselves, will move shortly afterwards.

- If you have a back way out of where you are that is not regularly used so unlikely to be watched as closely, sneak out and around to get close to the observation vehicle. At night this can be used for covert surveillance of the vehicle to see if there is anything further to add to your suspicions. The chances are that you will be detected doing this, but it will be enough for the team to assume their cover has been blown.

- Monitor the driver of the vehicle to see if he is being picked up nearby after leaving it, or has a secondary vehicle stationed nearby.

- Openly take photographs of the vehicle to scare it off.

This is also useful practise for vehicles that are stationed further along your usual route and may be part of a stakeout box that is waiting to pick you up once you pass. It allows you to confirm suspicions and possibly burn them depending on how close you get to them.

7.2.2 Rural

The rural environment offers far more opportunities to detect surveillance vehicles. The roads are narrower, more winding and have generally less traffic and more traffic hazards (road works, slow tractors) that play into the hand of the person seeking to detect surveillance. There are also opportunities to get off road and conceal much better, though it must be remembered that some of the pitfalls can equally apply to the target, especially when trying to escape surveillance.

On country roads, park up suddenly and watch the behaviour of the cars behind you. Ones proving reluctant to pass you are suspicious. It also gives you a good chance to have a look at any which are passing by and their reaction. Most people when stuck behind a slow moving car are keen to speed past and disappear when they get a chance – a tail is not so eager to be out of sight even if it is in front. When they have passed spin around and go back. If you don't go back, keep your eyes out for potential tails being parked up waiting for you to pass again.

Depending on what you are up to, when you turn your car around go a short distance again and park up once more. The tail having realised you have turned will turn and come back, so if one of the cars which passed you when you stopped initially passes you once more, you should be rightfully suspicious of them. This technique works best on roads with bends.

In rural lanes you have several options:

- Get out and walk up to a house or into woods, so forcing the command to give themselves away by following or abandoning you. Longer paths which allow you to get out of sight and double back are useful for seeing if anyone has pulled up and is waiting.

- Drive into a farm and turn around, giving suspect tails enough time to pass, then drive off in the opposite direction. If you know the area quite well, it means you can take a route that is hard for them to pick you up again.

- Use the narrow roads to your favour – the chances are that you will have all the surveillance team behind you, so effective use of traffic lights can lose the lot.

Finally, the chances are that if they are very interested in you, a simple transmitting bug (known as a "Bumper Beeper") is attached to the underside of the car allowing it to be followed at a distance. This is one reason why using your car to go direct to secure meetings or for high risk covert actions is not a good idea, as the chances are you will not locate the device.

Saying this, there are ways of testing to see if you have one, though not necessarily foolproof:

- Use a radio scanner to detect transmissions from the car.

- Drive into the countryside, park up and wait in an adjoining field to see if anyone comes along to check out why the vehicle has stopped. Tails picking you up when they really should not have is another sign they may be using a bug in this way.

- Stand next to the car with a friend and discuss a fake action to see if it provokes a reaction later on.

7.3 On foot

If you are being followed on foot again it is likely to use a team of people rather than an individual. Their dress will be nondescript and have few identifying marks or clothes. Saying that, ordinary policemen are quite easy to spot even in plain clothes by their walk, stance and general ineptness. With a more professional team, it is harder to spot surveillance as your line of sight to them is greatly reduced unless you spend a lot of your time looking behind you, which is not really recommended.

Passive detection

a. Enter a shop and watch who follows you or who waits to pick up on you again as you go out. Watch for people staring into shop windows. Often their body language will give themselves away as they are not doing it properly. It is useful to practise watching people in the street on how they window shop and such like before doing this so you can pick up the nuances that distinguish between someone doing it genuinely and those whose are attention is elsewhere (like trying to spot you). Check were their eyes are looking and whether they are doing more than simply staring ahead.

b. If the shop has a back entrance leave through it, and promptly stop around the corner to see if anyone else is looking rather hurried as they try to catch up with you. Look uncertain about the direction you are taking or look at your watch if you want to avoid being obvious that you are waiting to spot them

c. Stop at a cinema or theatre and read the boards there. This gives you an excuse to stop and look around.

d. If you go into a shop or an alley way you do not normally go into, is there anyone who crosses from the other side of the road you were on. Depending on what you have entered, what do they do? Do they follow or do they hang out opposite the entrance? If it is a small shop such as a newsagent or café then they are not likely to come in as it is getting to close to you unless they are interested in your shopping habits. If the shop or café has largish windows then you can use them to watch activity outside to see if anyone is loitering around.

e. Professional tails will be ready for you to duck into a shop or to do 'window shopping', so they will simply pass you by. Thus while you are looking for people also keep watch on those who have passed you by and then stopped.

f. In a café or similar chose the seat which allows you to view as many people as possible, and definitely face the door.
    - Keep an eye out for couples who are not chatting or not acting naturally. It has been known that while a group has been relaxing in a pub surveillance team members have come in and set next to them with bags containing listening devices. They gave themselves by their body language, consuming their beer or food slowly or not at all, and have very poor interaction among themselves, watching instead people from the group going to the bar or toilet, etc.

    - Is there an upstairs seating area with windows overlooking the street? This is a good place to sit and watch if anyone is loitering, waiting for you. Do suspect individuals watch the door to the café, etc., regularly?

g. In a bookshop is there anyone looking at the same books as you just browsed through, especially political ones?

h. On bridges and the like you can also stop to admire the view, again giving you the chance to look around you. Who does likewise?

i. Stairs and escalators in a shop give opportunities to look for tails. Approach them from the opposite direction so when you reach them you have to do a half circle turn, so able to look behind you without appearing to do it deliberately.

j. As you leave a shop, stop and ask someone the time or for directions, keep an eye on who might have followed you out, or is waiting nearby.

k. Chose a narrow or quiet street to act as a choke point to filter suspects out from the crowds making them easier to identify. Doesn't always work with a professional team as they will be prepared for this. If this is not a place you would go in the normal course of business then it becomes active detection.

l. If in a train or bus station, change position regularly and watch those standing still. Keep an eye out for people not reading timetables or newspapers properly. If purchasing a ticket, etc watch out for people standing right behind you who may be able to overhear.

m. In shops who is not actually shopping or appears out of place.

n. If approach a place you plan to use as your own observation point, check out who is already there to eliminate them from consideration.

o. In areas that are not centre of town or low on pedestrians in general do vehicles at stakeout points pull out and travel slowly behind you. More professional ones will move ahead of you and wait for you to pass.

p. Enter a place where an unprepared tail will look out of place, e.g. a punk shop, etc. If this is not an obvious place for you to be in then this becomes an active detection technique so hints at the fact you are watching out for surveillance.

q. As you cross a street who on the other side slows down to avoid crossing your path. Do they cross to the other side but continue in the same direction as you? At a junction who quickens pace to cross it before you do?

r. Given the increasing prevalence of CCTV cameras in towns, and not just in the centres, watch out for those which seem to move in your direction. With this, it is good to know where they are in advance and be discrete in your monitoring of them. If they do not think you are being aware of possible surveillance then they are unlikely to be discrete themselves.

s. Is there someone hanging around your street with a camera? This has been known to happen with amateur surveillance teams.

t. Shopping centres are awash with opportunities to put the surveillance team on their toes, as there are many observation points available as well as exits. Balconies are ideal for watching those coming in behind you, as are see-through lifts. If you can get into a lift fast enough you may have a get-away route through passageways to nearby buildings or car parks. Other tactics worth mentioning is to use little used exits to draw out who is following you; or enter shops at the last minute when it looks like you are about to leave. Standard procedure for surveillance teams is to cover all exits.

In some cases, though we are not aware of it being a regular practice, the tail will change their own appearance, usually with hats, glasses or coats, in order to allay your suspicions of them. Hence, focusing on these objects is not necessarily a good way to log the person in your memory as someone to keep an eye on.

Active detection

- Drop some paper (make it look like it accidentally falls out of your pocket as you take your hand out of it) and see who stops to pick it up.

- An empty street is a good place to spot or lose a tail. Try doubling back, watching for people walking past slowly and watching, etc.

- The main tool for detecting foot surveillance is the blind corner, and works very well with amateur or incompetent tails. Taking one you are setting up an opportunity to check reactions, by doubling back on yourself which they cannot see so are not prepared for, or by simply stopping and watching. If there is a café or shop with a good window just around the corner then entering that allows you to give them the slip or to observe their reactions. However, a professional tail will actually walk on rather than go round the blind corner, and use their communications gear to get another member of the team pick you up.

- When you go around a blind corner, consider ducking into an office block and concealing yourself there; this is worth doing if you are quick thinking and able to bluff receptionists.

- Double back on yourself, and repeat to see who you keep spotting. Tails will avoid making eye contact however, and will attempt to dress for the area they are in so it may not always be able to spot them. What you are looking for is the uncertainty that you have just caused them as they decide how to react to your change.

  A professional will be on the other side of the road rather than right behind you. Rather than just turning around, cross the road and then go back in the direction you came. This is active detection, but it is much better at forcing them to react and you have a good opportunity to gauge reactions. This is much more effective on narrow terrains such as foot bridges where there is not much of a gap between both sides and little traffic so you can get to the other side relatively quickly.

- Waiting in a queue for a bus is a useful method to spot tails and lose them at the same time.
  e. To spot the tail let a few buses go by to see who else is waiting (at the bus-stop or nearby) – particularly useful if someone gets on a bus with you when one going in the same direction has already called at the bus stop or train (if on a tram system or the London Underground).

  f. To lose them, you can suddenly 'realising' that a bus across the road is the one you want and making a dash for it is a good way of losing a tail and potentially exposing them. Alternatively, drop out of the queue as you are about to board.

- When you cross a street do people on the other side and double back in the opposite direction to the one you were originally traveling in are their people who cross the road to avoid you or seek to avoid eye-contact?

- A sudden and significant change in your appearance it can cause them to give themselves away as they try to check that they have got the right person still. For example, a dramatic change in hair style gave away several police tailing one activist as they all did double takes when the activist was picked up at the meeting point they were staking out.

Anti-Surveillance

On foot it is very hard to do this discretely unless you are quite lucky with the geography of an area and crowds. Busy town centres with lots of alleys and bending roads are easiest. Your best chance is to use established patterns to lull the surveillance team into thinking you are conforming, then seize an opportunity to disappear elsewhere.

a. Don't wear clothes, jewellry or hairstyle that stand out as these simply act as marker for them and means that they can be more discrete in tailing you. Surveillance teams focus a lot on clothing, so make it non-descript and common.

b. You can also bring changes of clothing and appearance (e.g. wigs) with you. Wigs are particularly effective, but only if they are cut to look good; badly fitting wigs only draw attention. As well as change of clothes have a second rucksack or bag to carry them in – avoid using the same one with different clothes.

c. Some quick ways to loose a tail are:
    d. Dash across a busy road the moment a gap appears. Use the opportunity to disappear down side streets or into any building with alternative entrances.
    e. Have a friend pull in and pick you up from a route where the surveillance team will not be following you in a vehicle. It may be that this can be done discretely with you hiding in the back under a blanket, but tends to work only where they are not expecting it and they are not familiar with the vehicle or the driver.
    f. Get lost in a crowd – a classic, but it does work. Factories and football matches are good for this as well as town centres, which is why it is worth knowing the area if this sort of event is a possibility.
    g. Shops with multiple and/or out-of-the-way exits are good for both active surveillance detection (wait next to exit and watch for people following you being startled by you waiting for them in turn) and anti-surveillance as it gets you out of sight long enough to get away. This works best with shops you don't go into, or if you do, you always use the same entrance and exit.
    h. Elevators that take you to other floors with exits are good; remember thought that the surveillance team will leave someone at the ground floor in case you return there.
    i. Places where there are security checks can work in your favour, especially where there are multiple exits, as surveillance teams will be reluctant to set off alarms with their communications gear. The delays for stop and search also play into your hands.

At night be prepared for the increased used of technology such as infra-red to monitor you.

Tip: Having traveled somewhere and then moved to being on foot, the surveillance team will also have one member watching your vehicle in case you return to it.

Remember, one or two coincidences are not proof you have a tail. You are looking for a whole series of them. Practising counter-surveillance techniques and developing your instincts will help considerably.

Public transport

Public transport offers a variety of opportunities for detecting and evading surveillance and makes life much harder for the surveillance team.

A professional surveillance team will attempt your destination and route, and monitor both as well as having someone on the same bus or train. This means, that depending on numbers they will seek to reach possible exit points to watch for you. If it is a public transport route that you use frequently, then will either follow the bus (something you can watch out for) or be waiting to pick you up at your destination.

However, if you use public transport regularly with established getting on and off points, then this can be turned into active detection or anti-surveillance techniques by getting off earlier or later and checking for reactions to make sure you have given them the slip. If the surveillance team has enough people then they will actually get off at earlier or later stops to avoid suspicion.

Jumping off at the last moment is a useful anti-surveillance technique as it forces them to lose you or expose themselves by reacting as well.

Beware of chance encounters with strangers, especially those who appear to have something in common with you, where some sort of rapport is attempted. Public transport is quite good for one-off encounters like this which allow them to get to know you better and evaluate your mannerisms. There is nothing to stop you lying about what you do, who you are, etc. If you have "coincidental" meetings again in the future it is worth being suspicious.

As you get off public transport or out of a terminal are there signs of surveillance vehicles waiting to pick you up.

Buses

If they do get on the bus then they will go as far to the back as possible so you will be kept in sight. A possible active detection technique is to stay on after the last stop and see who else is doing it – will only work if they are not familiar with the route otherwise they will not make this mistake.

Trains

a. Given the nature of trains then you are more likely to have a number of surveillance operatives get on and off the train at the same time as you.

b. The more you change trains the more it erodes the integrity of the surveillance team. Add to this by going to the barriers as if leaving then turning around and getting back on another train.

c. There are a number of exits for stations which you can use to your advantage, depending on crowd density and how well you can push through them.

d. A good feature of train stations (though it works well in other high density areas of pedestrians) is that there are strong flows of people in one direction. If you move against this flow, watch out for others doing likewise and struggling to keep you in sight. As you have to look as you do this, it is an active detection technique.

Night surveillance while on foot

This is a much different situation from day time foot surveillance. A professional team will be ready for it. Amateurs will not. At night when out an about, you are more likely to encounter a greater use of technology, for example night-sights. The fact that it is darker and quieter works in your favour since they need to get closer to keep you in sight and you can use your hearing more effectively. At night they are far more likely to use vehicles, especially when the weather is cold – loitering around outside when it is freezing is much more obvious to spot.

The best way to spot surveillance at night is to monitor for vehicles showing some of the following traits

3) Driving without lights
4) Lights going on and off in stationary cars
5) The sound of radio transmissions
6) Doors slamming shut as you approach
7) Vehicles parked in unusual locations.
8) Couples sitting in cars, staring straight ahead rather than engaging with each other.
9) Sitting for prolonged times with the engine running.

Surveillance teams have been known to use taxis and police cars in this situation. If you know your area well then you can spot them by being parked in places not normally used by them. For instance, police cars do not normally hang out in well-to-do estates. Taxis do not wait on poor and out of the way estates. People waiting on friends at nearby houses tend to park in the light and on the main road and not in out-of-the way places offering concealment.

Some tactics that work better at night are as follows:

a. If you think that someone is following you listen out carefully for the sound of their pace. It will be done to match yours, so as you speed up and slow down, then it will change to match. This is something you can actively hear.

b. You have more opportunities to conceal yourself and watch the reactions of suspect tails as they realize that you are not in sight. Remember, that if you confront someone then if they are innocent and will pretty much react in the same startled way, thinking you are a mugger. However, you can get up close and ask for directions, a cigarette light, etc which will put the suspect tail on the spot and give you a good chance to look at them, something they will really not like.

c. Taking blind turns at night forces the surveillance team to react more aggressively, so again forcing their hand if you are ready for it. However, given the darkness there is a possibility they will react more confidently if they think they have the upper hand.

Tip: Because it is much quieter at night it you become far more aware of sounds that occur naturally and it is easy to suspect every sound. In this sort of situation wait until you have actual visual confirmation rather than suspecting just noises.

7.3 Rural Surveillance

This is significantly harder to detect as the surveillance team will in general further away and there is much greater scope to hide, especially if there are thick woods nearby. A surveillance team will

- Wear adaptive camouflage.
- Be prepared for a long stay if necessary.
- Use infra-red and long range binoculars and scopes.
- Put motion-detector cameras in junk, trees and nearby structures.
- Take measures to hide the fact they were there such as dealing with bent grass and depressions.

Things to check for are

a. Repeated glints off binoculars from woods or copses.

b. Abandoned buildings where they are using to hide vehicles.
c. Transmissions from cameras.
d. Flattened grass and depressions; also vehicle tracks where they shouldn't be.
e. Identify potential observation points from your location and regularly check them – it may discourage the surveillance team from using them or getting too close.
f. Walk in an ever widening circle, looking for places of concealment focusing on places such as tree-lines, copses, thick bushes/hedges which have a view of the target area.

Having dogs around the place are particularly effective, and to a lesser degree motion-detector lights, though this depends on how covert the operation is.

7.4 Counter-surveillance

This is a phrase often used in the wrong context. It actually means using another team to monitor a target with the aim of detecting whether there is a surveillance team on them or not. A second group of people is much more effective than the target at spotting surveillance teams as they will have better lines of vision.

The trick to this is to set up a *check route*, also known as a *surveillance detection route*. In this the target and the counter-surveillance team plan out a route with gives the counter-surveillance team to set up in advance and able to watch for the surveillance team following the target. It is best done on foot routes as there are better opportunities for monitoring.

It is a simple idea but it requires considerable planning to be properly effective as there are a number of pitfalls for the activist:

- The surveillance team may be aware of who your friends are so will be able to recognize their faces; if engaging in this sort of operation, consider some sort of change of your normal appearance or disguise.
- The security around the set-up needs to be very tight – if you are meeting up to plan it, the meeting needs to be tight so that the surveillance team doesn't get wind of the idea so be prepared.
- The counter-surveillance team needs to be able to move swiftly and discretely; this includes hand signals that are not too quick so others can pick them up (eg, outstretched hands as opposed to a quick scratch of the chin).

However, it is important that this is not done in a way that alerts the surveillance team that there is a second team also working. If the surveillance team thinks that it is under surveillance the chances are that they will discretely withdraw and come back another day instead.

In theory there will be no contact between the target and the counter-surveillance team; however, having a friend meeting you and stopping to have a quick chat offers both target and friend to scan the surrounding area for suspects.

7.5 Blatant surveillance

Much of what has been said also applies to being chased. Where it does not apply to when being followed by someone rather obviously primarily to intimidate or make actions difficult as in mass public actions. In this case you simply have to give them the slip. Be unpredictable, use public transport and some times just run (that is not illegal so it is not grounds to stop you, though that may not bother them). It depends on the situations, whether you publicly burn them to people around you, or discretely lose them.

The other approach is to be completely innocuous such as having a coffee or a pint or simply shopping. Having to wander around the female underwear section of a shop puts most people off – especially if and do something you confront them in a socially embarrassing way.

8. Computer Security & Internet Privacy

A detailed guide to computer security is an entire handbook in itself, and once published would promptly be out of date. Though the security issues are not moving as fast as they have been, the technology is always changing. Many of the old guidelines are simply outdated now and becoming little better than myths.

Nevertheless there are some pointers that hold through and you should be implementing. We list these below. As a basic secure system we recommend a computer running Ubuntu/Debian Linux using the Firefox internet browser and Thunderbird for email. Email should be encrypted as much as possible using a combination of Enigmail with GPG (a freeware version of the renowned cryptographic programme PGP - Pretty Good Privacy). Finally, use disk encryption to protect your sensitive data. For anonymous web browsing install the Tor software suite and the FoxyProxy add-on for Firefox. That's it in a nutshell.

Though we are generally brought up to use Windows as the basic operating system for our computers, there are other options out there, and from a security point of view they are way better. Apple Macs are better than Windows, but Linux is the best, in

particular user friendly distributions based on Debian such as Ubuntu. The way Linux is set up makes it inherently more secure than Windows / Macs and it is not as user-unfriendly as it once was.

Even if you are not prepared to make the move away from Windows or Macs, much of the software we recommend (Thunderbird, Firefox, etc) comes available for these operating systems, and is a good step forward. They are all free as well. You may have to do a bit of research but the software has come on leaps and bounds in the last ten years in terms of usability and ease of install.

A problem with computers is that their guts tend to work in strange ways and you do not know what they are up to all the time. In particular they store information in odd places, unencrypted in swap spaces and so on. The precautionary principle is always best.

All of this technology is free and relatively easy to install these days with a little bit of work.

8.1 General tips

h. Keep your computer up-to-date, installing the latest or next-to-latest versions of software. Make sure you are doing this regularly.

i. If running Windows/Mac, install various anti-virus / anti-malware / firewalls software. This can be done individually or there are programmes that do most of this (eg. AVG, Norton, etc). None of this is worth anything if you do not keep it up to date, so ensure that your Live Update features are enabled and working correctly. Do not open or answer spam. There are many online sites which give up-to-date advice on the basics of security your computer so check them out first.

j. Login. It is always good to have a username and password for your computer. This will not stop those who are determined to break into your computer as it is easy enough to boot around them; however, it will slow down considerably the causal spy or other nosy individuals. It is worth creating multiple accounts on your computer for the different aspects you use it for, so it is not clear which is

k. Turn your computer off! Never leave your computer on and unattended, open for everyone to use. If going away for a short time, then use the screen lock feature (consider having an automatic lock if the computer is unused for say more than five minutes). Anything longer or overnight, then make sure to turn it off properly. There is no point in being raided and various dubious information and passwords are cached in a computer they now have complete access to. For similar reasons, it is better to power down your computer rather than panic and pull the plug-socket, especially where you have disk encryption.

l. Multiple Users. If there are more than one of you using the computer create multiple accounts so they cannot see your work. It is also worth creating unaccredited accounts in general names for sensitive work so it is not in any one's name.

m. Passwords. Chose passwords that are effective, Password protected computers are not secure to the prepared infiltrator so encryption of anything sensitive is a must.

- i Do not base them on the names of family, pets or dates of birth.
- ii Include non-dictionary words or sequences of letters/numbers which are essentially random.
- iii Really sensitive material should be protected with passphrases of a minimum of 16 characters from the entire range available – including upper and lower cases, numbers and any permitted symbols.
- iv Change them on a regular basis.
- v Do not write them down and stick them under your chair or desk – these are the first places that an intruder will look.
- vi

n. The Physical Set-up. Consider the external threats to your computer. Could it easily be picked up and walked out. Given how many computers are seized a simple solution to imped this is to have it chained down to a desk or wall. Be careful about the screen facing windows - could someone with a good camera/binoculars read what you are typing. It is best to have computers facing away from windows, and if typing sensitive stuff keep curtains closed.

o. Wireless. The problem with wireless is that it transmits in all directions at once, so anyone able to intercept your signals can see what you are doing. This goes for keyboards as well as routers, so were possible we recommend using cable to connect up the various parts of your machine. If cable is not an option, then make sure that the encryption on your wireless is up to the job - a lot of encryption standards being used such as WEP can easily be broken.

p. There are a lot of rumours and myths in computer security, more so than in other areas of security. Most can be discounted based on poor understanding of the underlying software or simple scaremongering. If in doubt check out

reputable sources, but do not stop using something simply because a friend of a friend of a friend once read an article, etc.

q. Open source security software is generally more trusted than proprietary software because the code is freely available. This means that it can be peer reviewed and checked for flaws/bugs in a transparent way. There is also a good history of where there are flaws of making updates available faster.

8.2 Encryption

Encryption is the process of encoding your data so that only you or others that you have selected can open it. It comes in many varieties, but there is only one we recommend at the moment and that is the paired public-private key method as used in the renowned PGP programme and others.

In this type of encryption, you create a pair of keys, a public one which you can give to anyone else and a private key. The public key is used to encrypt the information for your eyes; however, it cannot decrypt it. In order to do that, you need the corresponding private key.

The private key you never see, it is kept on your computer securely locked up behind another layer of encryption which can only be accessed by a passphrase which only you know.

This means some, including yourself, can encrypt stuff for your eyes using your public key, but nobody else can see it other than yourself. It is a tried and tested system and is known to work very well. Suggestions that it can be cracked by computers are way off base - everything can be cracked eventually, but only if you have all existing computing power in the world running on the problem for several billion years. Its not going to happen.
The main weakness is the human one - it is only as good as long as your passphrase is undiscovered, so it is vital that you do not write it down or chose something relatively easy to guess. If you are exchanging emails with other people then it is even more important you get this right as if you are being sloppy on your password then you are putting them at risk. As noted, minimum of 16 characters drawn from upper/lower cases, numbers and symbols, preferably including non-dictionary words and random patterns in it. Make sure you can remember it as if you forget it, then you do not get your data back.

The recommended and standard encryption package is PGP (Pretty Good Privacy - www.pgp.com) which is well established and has sustained the test of time. We know of know successful attempt to break its intrinsically, though it can be broken by poor implementation or using weak passphrases, though both these are issues we can do something about. As well as a good passphrase, it is also worth choosing a key that is as strong as possible - we recommend a key length of 4096, which will defeat any attempts to crack it by brute force. This is why organisations such as MI6 use PGP, and the US government spent a lot of time trying to stop it spreading world wide.

PGP is no longer free open software, though older versions which are can still be downloaded from www.pgpi.com. However, an open standard known as GnuPrivacyGuard (GPG) has been developed and can be downloaded from www.gnupg.org. In Linux it needs to be used in conjunction with an interface such as GPA or Seahorse. PGP / GPG will encrypt both emails and files. For the former, see below. The keys used by both programmes are in standard format and can be used by each other so avoiding problems with incompatibility.

A good guide with images to setting up PGP in Windows is at www.shac.net/pgp.index.html

Tip 1: It is good policy to change your GPG keys on a regular basis - say once every six months. This means that even if one key is compromised the rest of your material is not. Though if you have archives remember to keep a back up of your old key or you lose it all.

Tip 2: Alternatively, one way to make sure that no one can access your data is to destroy your private keys. If these do not exist then it is impossible to unlock it, by your or anyone else.

8.3 Data Management

Once you have set your computer up to be secure your next job is to consider how you are managing the personal and sensitive data on it. Ideally, you will have this behind password protected accounts. However, it is not enough to stop there as if your computer is seized then this is easily circumvented.

a) All sensitive information should be encrypted (see next section) with GPG or PGP level encryption.

b) Sensitive information ideally is kept (encrypted) on a memory stick or portable hard-drive which is stored elsewhere from your computer. Its been known in raids for police to not recognise such hardware as they focus on stealing activist's computers.

c) Make backups of your encryption keys and important data and store them somewhere other than your house that is not likely to be raided or stumbled across. There is no point having your information in your house if it is only going to be seized as well. Likewise, no point having encrypted files if you do not have the keys to decrypt them (even if you get your computer back the police might delete your keys). Ideally, you will have backups of your keys in one place and your data somewhere else.

   A useful tip is to compact your files into an archive before encrypting them - this means is that even if the state gets access to your files they cannot even read the names of the files, or discern what sort of stuff might be in them.

d) It is best to have your encryption keys stored on a memory stick and not your computer.

e) Windows and Macs allow files to be recovered as the delete function only partially removes them from the computer. They also store bits of files in different parts of the memory. This means old files can be extracted if they are simply sent to the trash. To get around this you need to wipe files using a dedicated programme to ensure files are properly removed from your hard-drive. These programmes often have settings for the number of overwrites which erase the data - this should be set to between 7 and 9; any more is overkill and more likely to drastically shorten the life of the hard-drive. Discount rumours that say you need to do more than this. As well as wiping files directly, it is also good to do free space wipes on a weekly or monthly basis to make sure all floating fragments of data are removed.

f) The best solution is to use disk encryption. This software allows part or all of your hard drive (or other storage media) to be encrypted and comes highly recommended. It means when your computer is seized then they cannot access the data on it at all. It helps eliminate problems with file fragments and deletion that have recently come to light in various cases. Two free disk encryption tools are at www.truecrypt.org and www.freeotfe.org Take your time to understand how this software works.

g) Do regular clean ups - get rid of or securely archive incriminating stuff you do not need, even if it is encrypted on your hard drive. Delete old emails as a matter of course.

8.4 Security across the Internet

As with computers the internet and the security/privacy issues related to it have changed dramatically over the years. Some things have remained the same, which boil down to that if you do not take care to obscure your tracks or encrypt your data then it remains open for a whole host of people to access.

Monitoring internet activity is as trivial as it is with phones. All internet traffic, whether emails, instant messaging or web browsing involves sending data through various servers and at any point in between this can be picked up and read. Due to the nature of the network, every computer online has addresses (known as IP addresses), which even if they are temporary, can be combined with the logs of Internet Service Providers (ISPs) to identify people. In the UK and elsewhere governments are requiring ISPs to keep logs of activity and emails for six months, so everything you are doing is not only being watched but recorded as well.

The basic message is that unless you are taking precautions, you need to assume that everything you are is watched and open to being monitored.

8.4.1 Email

8.4.1.1 Encrypted Emails

Email is as secure as sending a postcard unless it is encrypted. As already noted above, we recommend only using GPG or PGP, though for the rest of this section we will only discuss the free, open GPG version

When using your home computer the Enigmail tool allows it to integrate seamlessly with Thunderbird for ease of sending encrypted email. Depending on your set up it can also integrate with other email programmes. A useful feature in Windows is having PGP in the Windows Systems Tray (normally at the bottom right hand side of the screen) which allows you to encrypt clipboard text including the messages in webmail pages.

However, GPG is only as strong as the weakest passphrase so take care - if the person who you are communicating with is not using a strong passphrase or has a compromised machine then you're emails to that person are vulnerable, so even if you are using encryption take care what you are saying. For highly sensitive discussions, GPG is best for setting up secure face to face meetings were you can take other precautions to ensure your privacy.

One fear is that using GPG / PGP marks you out as someone who needs to be monitored, so therefore it is safer not to use it. Unless you have never appeared on the states radar and has never connected with some who is, and are careful not to say anything that might trigger some the monitoring software, then this is a false premise. It is more important that individuals get

used to using encryption software for even trivial things so that those who depend on its privacy are able to use it as cover. Using encryption software for emails is not illegal in most countries.

8.4.1.2 Other Encryption Solutions
There are other protocols for protecting the privacy of emails. In modern email programmes there are options for using SSL or TLS to send emails. These mean that the emails you send to your email server are encrypted. The problem is that once they leave the server on the way to somewhere else they back again in plain text.

Saying this, there is a move now towards something called SmartTLS which allows for end to end encryption between email servers so no email is ever sent in plain text. This has now been adopted by many of the activist tech collectives, so email from, say, a riseup.net email account to one at mutualaid.org will be fully encrypted all the way.

8.4.1.2 Email Identities
Most programmes allow you to set up multiple accounts to send messages from, so you can use different identities for communicating with people. This will not confuse the security services who can track you via the headers hidden in all emails, however, it is often useful for approaching companies or doing research.

Remember, you do not have to give your real name or other details. Use other names / create separate identities for mailing lists, etc, but if you are setting up separate identities do not compromise yourself by using ones which clearly link back to yourself.

It is always worth avoiding emails that link you in with particular campaigns or set out your politics too much - think how your email address would look to a judge?

8.4.1.3 Webmail
Other options are to use webmail only as this means there is little stored on your computer to link you directly to the email account, though any email will log the IP address of the computer it was sent from which may link back to you. This is a better option for public computers.

A problem with a lot of webmail accounts, eg. Hotmail or Yahoo, is that only the initial part is encrypted, the bit where you log in. After that it is no longer encrypted and open for others to monitor it. However, many of the activist tech collectives who provide email services are providing fully encrypted email sessions to help deal with this.

We note that RiseUp.net now allows you to encrypt your messages using PGP via webmail. This is a very nice step forward as it allows you to use PGP from public computers which was awkward in the past. PGP messages can be sent from other webmail accounts via public computers, but often you need to create the message at home, encrypt and save it to a USB stick or floppy, and take it with you to a computer which could accept removable media such as this.

Do not rely on Hushmail; their claims that not even their staff can access their emails is not true as the following article demonstrates: http://www.theregister.co.uk/2007/11/08/hushmail_court_orders/ Hushmail has provided decrypted emails in response to a court order. More detail about this risk and it's extent can be found here: http://breakallchains.blogspot.com/2007/11/hushmail-open-to-feds-with-court-orders.html It does not help either that Hushmail's software is also secret so users are still trusting their claims as regards to security.

However, Hushmail does still have its uses in sending one off emails and also for dead letter drops due to the encrypted connections to its servers.

The old remailer system is pretty dead these days or compromised, sadly.

8.4.1.4 Dead Letter Drops
These are an adaption of an older form of communication. A email account is set up and the details shared by hand between a group of people. Logging in from public computers, you can leave messages and files for each other in the drafts folder without ever having to actually send emails.

It can still be opening for monitoring, but if there are no reasons to attract attention and nobody uses other peoples names then it is a fairly secure method of communication. Remember to delete old material once dealt with, and if compromised someone will have to delete the contents altogether.

8.4.2 Anonymous Web browsing
As with email, your IP address identifies you to every website you are visiting and to anyone watching in between unless you take steps to anonymize your browsing.

As with emails the way forward is to have encrypted connections between you and the rest of the world. You know you are on an encrypted connection if the web address starts https:// rather than http://. The more up-to-date browsers show if you are accessing a secured website by little icons in the bottom left hand corner (highlighted key, closed padlock etc) or by colouring in the web address line. To see what your browser looks like check what happens when you log into a webmail account.

From home, the safest way is to use a proxy with encrypted connections - these are computers that stand between you and the rest of the internet so the end pages only see the last intervening computer and not you. The simple way to do this is to use the Tor system - see www.torproject.org. We will not go into the details of how this works here, other than to say that is a widely used system for protecting privacy of those using the internet and the more who use it the better.

To go with this there is a Firefox add-on called FoxyProxy which simplifies matters considerably.

However, you still have the problem that if someone has access to your computer already via key loggers, etc they can still be watching everything you do. Likewise, if you are doing personal stuff at the same time, eg logging into your easily identifiable email accounts then you are also giving yourself away.

There are a number of solutions such as online sites that let you browses through them, but they are generally very limited in usefulness - most will not let you use webmail or do not have encrypted connections, so all they are useful is for visiting websites which you do not want the end user to know your IP address. To do more you have to pay which defeats the purpose of anonymity.Tor will do this and more without putting you in the hands of dubious companies running the anonymizing websites, for free.

For more serious stuff it is still recommended you find a public computer somewhere.

8.4.3 Public Spaces

Internet cafes, public computers and HotSpots are all useful places to browse the web or send emails from. Many have poor logging or monitoring, and large computer arrays make it harder to pinpoint people. Storing stuff on line in anonymous accounts can be a good way of protecting your data and yourself by having nothing in your home - ensure though that you are using encrypted communications as much as possible.

However, they do have some risks associated with them:

a) CCTV is common in many public places and internet cafes. Adopt the techniques noted previously for handling it, such as baseball caps, not looking up, etc.

b) Larger places will keep records of activity on their computers; or have system admins who can read everything you are doing on the computer. Bored staff have been known to read and congratulate people writing up action reports

c) Watch out for people behind you reading over your shoulder.

d) Give the mousse and keys a quick wipe down when you are finished, and pay in cash.

Some tips to increase your security using public spaces:

(i) With internet cafes select those that are not part of a larger chain. Often small places in areas with large concentrations of migrants are good places to go to.

(ii) When using HotSpots for WiFi access select areas such as trains, cafe's offering free services for increased anonymity. Again be aware of CCTV inside and outside. If using your own laptop change the identifier for the session, then change it back again.

(iii) If doing sensitive stuff, do not send personal emails at the same time, or log into accounts connected to you or you will compromise the anonymity of your sessions.

8.4.5 Publishing Websites

A common question is how to publish websites safely. It is not easy unless you are prepared to throw money at the issue. The expensive solution is to buy space on some of the foreign hosted services that are focused on privacy so nothing is ever registered in your name.

A problem of doing stuff yourself but having your website hosted abroad is that you may still be liable, depending on the laws of your jurisdiction, for the contents of the website as its publisher. Also, if your opponents bring a lawsuit against you in the place where your website is hosted you are going to find it very difficult to defend.

A cheaper and easier way to do it is to use online blogging services such as wordpress.com which have a good record of civil liberties (though they also often host assholes as well). Advantages of doing this is that websites can be edited and created in internet cafes without ever having to do it at home. However, it gives you much less control over the design of the website.

At the same time have a colleague in another country buy the domain name (ie yourname.com, etc) and have it redirected to the website every time it gets taken down. You can have your website mirrored in a whole range of different places, and all you have to do is change were the domain name around, which is far easier. Use a googlemail account to go with it, or something similar. Free online hosting services are useful, but on the whole they are fairly weak when it comes to resisting legal challenges. If you need something more stable and that does not get blocked so much by webfiltering software, then look at hosting in Holland, Sweden, Canada or some of the far eastern countries, and ask some of the activist tech collectives that are available.

Be aware though that foreign hosted sites are not immune to the forces of the law - various treaties mean that police in once country can act on behalf of those in others in taking down servers.

8.5 Conclusion

Computers and the internet are great tools that have transformed activism immensely. On the other hand they are hi-tech solutions that carry many risks as well. Make sure that you set your computer up right and spend time getting to know it. Modern computers are fast enough that most security measures will not impact on their performance, but be prepared for some glitches and slowness - it is one of the prices to pay for knowing you are safe. It only takes one slip up to start compromising everything as due to everything being recorded on the internet there is far less slack in the system to slip through. Especially as private investigators and the police are becoming far more clued up on computer forensics. In the last couple of years there has been a pronounced growth in the state's general experience in handling computers and knowing what to look for.

A serious danger with computers are "keyloggers". These can be both software and hardware which record everything you do, and can be programmed to look out for stuff such as passwords, credit card numbers, etc. The FBI used these to record the PGP passphrase of a member of the Mafia and thus break into his emails (one reason for changing keys and passphrases regularly). However, if it gets to this sort of level then you need to be rethinking your security and your relationship with your home computer.

9. UK Legal Issues

The first important thing to remember is that it is not illegal to protect your privacy or your security. A court or police may draw their own conclusions on your behaviour, but there is no law to stop you taking preventative measures.

Likewise, it is not illegal to keep your actions anonymous, whether sending letters or emails, or attending protests. What could be illegal are the contents and intention of the message/protest.

Know your law – it will keep you from getting convicted (if not arrested) and by knowing your rights you can protect yourself much better when you are approached by the police, or being searched (both personally & at home). For up-to-date information on the state of play with law in England and Wales visit www.freebeagles.org or www.activistslegalproject.org.uk. If you are based in Scotland then the law is different – check out
http://g8legalsupport.info/2005/03/08/an-activists-guide-to-scots-law and www.tridentploughshares.org.uk

Keep an eye on forensic issues & standards of evidence in court. This can be picked up from news stories of high profile convictions and also websites. Knowing this will inform how you decide when balancing up risks.

9.1 Regulation of Internet Powers Act (RIPA)

After several years of delay the UK Home Office has now enacted Section 49 of the RIPA, whereby the police can demand the passwords to your computer and any encryption techniques you are using in order to read your data. Failure to provide them could in theory result in a five year prison sentence. A number of people have been changed with not surrendering the details though not any political activists that we are aware of today. Of those charged we are not aware of any trial having taken place at the time of writing.

In practice it is potentially unworkable as it is hard for them to prove that you have not actually forgotten it:

- through the lapse in time since you last used it;
- as your password was fiendishly hard to remember in the first place;
- from the trauma of the raid when your computers were seized.

This issue has yet to run its course so it is not yet possible to state the fall out from this. We think the law remains open to being challenged in the higher courts where it might conflict with the Human Rights Act, and both practically and on point of principle it is worth activists refusing to surrender their passwords.

10. Talking to others about security

It is important to discuss security in your group. You need to make sure that your affinity group or organisation can be trusted to look after itself, and that weaknesses are minimised according to the threat you are likely to face. However, there are several pitfalls here you need to watch out for.

I. If you go over the top, then you risk putting people off, scaring them or otherwise disempowering them. Encourage people in your group, especially those less experienced than yourself, to think about their security needs, and how lapses in security can affect other people but don't enforce without explanation. Be wary of letting a 'more-secure-than-thou' competitive attitude develop as in a group as that is very off-putting; likewise with installing a paranoid mindset rather than an active one.

   As you develop the security mindset, it is easy to lose understanding about how people who are new to the scene think. Do not oppress them for getting things wrong, but do suggest where they can make changes. Explain to them why you carry out certain processes, and encourage them to ask questions – otherwise they'll never learn and you could be jeopardising yourself. Don't panic if new people start asking about security and other issues; it's how people learn and develop. If you are not going to provide an answer, explain why without being condescending.

II. If you see a security lapse in someone else, there are several ways of dealing with it:

   1. Bring it up as a general point at a meeting in a sensitive manner without particularly naming and shaming. This has the advantage of reminding others of their responsibilities as well. Shouting and ranting is not beneficial to anyone.

   2. Take the person aside and explain your concerns, explaining that you feel uncomfortable and why. In particular, say that it is you who feels at risk. If they do not sympathize with you they are less likely to pay heed to your request that they improve their security so let them know that you will have problems with working with them in the future. You can also ask others whom they may have higher respect for to also approach them.

III. Don't boast about your own security precautions. Security by obscurity is not a sensible approach; however, using obscure ideas to improve on your security is a useful technique, but only works as long as it remains obscure.

   Beware of your own ego on this one. You can suggest techniques in general, but the actual bit of cleverness, keep that to yourself. For example, if you use Finnish for your password, you can maybe say that you use a difficult foreign language; just don't say which one.

IV. Don't give bad advice, or make things up rather than appear ignorant. Security can change quite rapidly, especially with scary developments like RFID chips, improved biometric techniques, etc, so if you don't know the answer then it is better to say so, than to lead someone into a false sense of security.

V. Watch out for people who are not acting as securely as they claim to be; the question then is if they are prepared to lie over one bit of security, then what else are they allowing to lapse. Give them a chance to change, but if they don't, then take precautions to ensure that they do not end up compromising you.

All this aside, just because someone is not at your level of security it does not mean you should never trust them. They may not know all the ins and outs yet. An action, especially a low-level one, can be an ideal time to teach by example up and coming activists what they need to be doing, while at the same time actually doing something to justify it all.

11. Future shocks

As technology develops, there will be advancements in methods of forensics, of biometric identification of people, and also in tracking devices. These are the three main worries activists have in terms of security. However, there are pros and cons here, and don't believe the hype.

Biometric recognition techniques – such as face recognition technology - are proving not to be as good as claimed. With face recognition, the problem is that there are two many false positives, that is, too many people are being picked out as possible suspects compared to the actual number of suspects there is. This somewhat contradictory situation means that not as much is gained from this technology as hoped as users of it have to spend as much time dealing with the false positives as following up on the genuine leads.

Saying that, CCTV is improving widely in quality and also in distribution, and now beginning to include microphones.

The police do not have all the technology they make out to have. In the UK, technology comes through a non-public body called the PITO (Police Information Technology Organisation – www.pito.org.uk), which evaluates and buys in new technology for the police to use. So when it is trumpeted that the police have a new technology, what it really means is that the PITO have got it, and not necessarily individual police forces. They have budgets to adhere to, so try to buy in the stuff they really need, meaning a lot of the fancy hi-tech stuff is actually ignored by the majority of forces.

The main changes of relevance to activists are:

g. Improved forensics catching traces that would have been missed on materials, etc previously.
h. Improved data exchange between police organisations and between the police and various other keepers of personal information such as banks. This also includes improved processing and cross-referencing of information (see also the risk of compulsory ID cards).
i. Increasing sophistication of listening and tracking devices, in particular in transmission range and in miniaturization of them (eg RFID tags). Though the technology has been around for some considerable time, it was not always practical for security agencies to use them – for a start they were more easily picked up by the activists. This is changing.

However, there is hope – and it comes in the form of budgets. The promise of hi-tech equipment and techniques is as much about saving costs as it is about effectiveness. As security agencies come to rely on them, they will rely less on low-tech and manpower intensive techniques (such as active surveillance).

The result is that low-tech security precautions can actually become more effective – bugs only work if they can be placed somewhere you are going to be talking; using ATM machines and credit cards to tag you cease to work if you pay only in cash. This is why we are confident that activists will continue to be a thorn in the side of the status quo despite constant oppression from state and corporations.

12. Closed Culture vs. Open Culture

What we have written in this booklet is very much for an activist culture quite closed in nature. Other groups prefer to go for a completely open approach, not hiding what it is they do. We are not opposed to this, and on some levels it is an advantageous route to go down.

Where the open culture works best is on the legal and large-scale approaches. On smaller scales and for covert actions problems will arise. It is a particular risk, when everyone attending an overt action does not have the same agenda, and someone may do something (eg a brick through a window) which leaves others in trouble they were not prepared for or had not signed up to. Of course, by having a large meeting, it is much easier to get everyone singing from the same sheet, so to speak, but this is not guaranteed.

Larger meetings make it harder for infiltrators to be picked out as well and on the organisational front are a nightmare to keep quiet – this means that they tend not to stay secret for very long. The basic rules should be that all mobiles will be switched off and that journalists are asked to leave.

It is important to be inclusive, but at some point it will become a risk; having as many people as possible at an action is not helpful when this approach means that the action is effectively scuppered by your opponents. The more successful you are as a campaign or activist group, the more this will be come a problem. Where larger meetings are fine for overall strategy, tactics for individual actions are best left to smaller groups working away quietly away from public glare.

13 Writing letters

Even writing letters can get you in trouble these days if you are not careful, especially when companies and the like can afford their own DIY DNA-testing kits and the like. There are quite a number of things you can do, all legal, which will help maintain your privacy. Below is an account of how one person writes letters to ensure complete anonymity. Not everything they do is necessary - play it to your own needs and situation.

13.1 Writing letters at home

Preparation is everything. It comes in two stages: acquiring the materials, and preparing the writing room. Material is purchased out of town from well-known shops, buying the most popular brands, in particular generic shop brands. Everything is bought in plastic wrappers so they are not directly touched. At home, they are kept separate and the receipt burnt.

At the hotel or home one room aside for the purpose and given a thorough clean to remove as much stray hair, dandruff, skin cells, etc. The table is washed down and disinfected (cheap vodka or white spirits will do); the floors hoovered and the walls dusted. Any animals are kept out. Shower, and put on freshly washed clothes, or even a paper suit. Wear long sleeves, and give hair a good brush, tying it back if necessary.

When writing put on a new pair of washing up gloves before doing anything else, such as opening the pens and paper. All wrappers are kept in the shopping bag for disposal of later. Paper is very good at catching fingerprints, so it is important to keep your skin away from the paper.

When writing, don't lean over the paper, breathing on it. Form the letters carefully taking your time over them if necessary. The faster you write the more likely it will look like your natural handwriting. Watch out for examples in your letters that act as tell tale markers, like how you form the letter G's. Don't be afraid to start over again. If you sneeze or cough, scrap the letter and wipe the table down again, as it will spray the area with your DNA. Don't forget to burn the discarded letter later.

Alternatively, buy a second hand printer and new cartridges to write it on, but dispose of straight after, taking care to destroy it first.

Likewise when addressing the envelopes. For sealing them, many envelopes nowadays are self-seal. If not, then use a wet tissue to glue the envelope shut. Put the envelopes into a clean plastic bag for posting, as soon as you have finished them (so if you sneeze or do something like that, then these will not have to be scrapped). As with envelopes, use self-adhesive stamps, buying a new lot in book form.

Post out of town, trying to use a different postbox each time, preferably ones not in town centres where there are CCTV cameras. Countryside ones are good. To avoid getting fingerprints on the envelopes as you post them, use the plastic bag to dump them in the post box (doesn't look as obvious as gloves in warm weather).

13.2 Computers, printers & photocopiers

13.2.1 Computers

On the computer, use simple text editors such as NotePad on Windows, SimpleText on Macs or emacs/vi on Linux. Big programmes such as Microsoft Word, Lotus Notes, etc often store backups of your text, and have a variety of issues that you would probably want to avoid, as if your computer should be stolen, others may find it easier to locate the letters you have created. In fact, we would recommend that you avoid Micro$oft Word altogether.

Where possible, do not save the file; some systems will allow you to print off a file without saving it first. With the simple text editors this means that you can avoid leaving traces on the computer, as the text will only be held in the working memory.

If you do save the file, never simply delete it as this does not actually remove it from your computer. Instead use a dedicated wipe programme such as PGP Wipe or Clean Disk Security to remove it fully from the hard drive. Better still, if saving it, do so to a floppy disk that can be burnt if necessary. Make sure that the number of wipes is set to at least 8 or 9.

Finally, if writing something of a particularly sensitive nature then use the free space wipe options in the above software to be on the safe side. It is good practice to run free space wipes regularly to make sure that there is nothing awkward left behind on your computer disk. Though be aware it will shorten the life of your computer's hard drive.

Alternatively, if the environment is safe enough, then use a university or library computer, so there is no connection to your home computer. If you are technically skilled, consider using free (or crackable) WiFi hotspots on buses, trains, coffee shops, etc (though change your computer's identifiers so it can be traced back to you if your laptop gets seized

13.2.2 Printing

Printers and especially typewriters have their own fingerprints. This means if they suspect you wrote a letter and they get hold of your printer/typewriter forensics can match the two up. There are several ways around this. One is to use a printer shared by a large number of people. It is then far harder to connect you directly to it. You can type the letter up at home, and bring it in on a floppy disk. Some problems with this are people looking over your shoulder so check out your situation. It is good to have several windows open on your screen if you are working on a public computer, so you can quickly bring another to the front, hiding what you have been typing.

Secondly, when you are printing out you do not want to touch the actual letter or have others see it. To avoid the obvious wearing of gloves, if the printer is relatively quite, what you should do is do a print run of a couple of things at the same time with your letter in the middle of it. This means there are pages above and below it that you can catch it in between with, so you can avoid actually touching the letter itself. Alternatively, if the printer is busy, put in a page or two of garbage text at the beginning and end of your letter to achieve the same effect.

13.2.3 Photocopiers

Finally, once you have your letter printed off, a very good technique to adopt is to photocopy it. This will help avoid telltale printer marks by obscuring them with the photocopier's own fingerprints. To enhance this, put the page on the printer at a slight angle, alter the contrast a little and maybe put the photocopied version through again to increase the blurring effect even

further. Remember to burn the originals when you are finished with them (do not simply put them in the nearest bin). If possible, go to a different town to do the printing and photocopying.

14 Using Mobile Phones

Activists have conflicting opinions on the risks associated with mobile phones, ranging from considering the security risk from them to be negligible, to keeping them at arms length as much as possible. The lack of solid information about mobile phones has bred a variety of myths, easily dismissed by those with less to be concerned about. We, however, recommend erring on the cautious side as can be seen from the information in the rest of this section.

In November 2006 one of our collective attended an industry workshop on mobile phone security with special relevance to activists. Among the key speakers was a mobile phone security expert who works with a wide range of corporations, including the police. His advice was that for all our worries and fears we have about mobile phones - it's worse than we thought. When it comes to activism and mobile phones, leave yours at home. We consider that good advice. Like everything there are exceptions, but with mobile phones good practice is to treat them with the utmost suspicion from the start.

14.1 Inside a mobile phone.

A mobile phone is a complicated beast, and is getting ever more so as technologies converge. From a hardware perspective, there is the

a) the battery
b) the SIM card
c) the phone itself

The battery is the main power supply for the phone. People often recommend removing it so the phone will not work. This is not necessarily the case. Some models carry secondary, slimline batteries to keep some functions going. How effective these are at maintaining the phone as a listening / tracking device is a matter for debate, but again the advice from those in the know is that taking out a battery is not good enough. Looking at the increasing miniaturization of bugs in general it would seem to us that even a small secondary battery could allow others to use the mobile phone as a listening device.

The SIM card is a small chip which carries various details, in particular the phone number itself. It is a relatively simple bit of circuitry easily removed from the back of most phones.

The phone is a complex bit of electronic gadgetry that performs many functions, but includes microphones and listening devices in their most basic forms. More modern phones will have camera features and amount to small computers in their own right. Each phone carries its own serial number called the IMEI number. This can be changed, but in the UK that has been made illegal in an effort to deter phone thieves.

The other aspect to a phone is the software. Since the beginning of phones, various manufacturers and networks have included software in addition to the advertised features. A phone is a small computer, and the more they develop the greater their sophistication has grown, so that more and more features can be added. Each model is different, and nobody can say what is exactly on a phone, as the manufacturer (eg Samsung, Motorola), the Network (eg O2, T-mobile, Vodaphone) and the final vendors all apply their own software, and that too will vary from model to model, and from country to country. Basically, there is a lot going on in a phone that we might not have a clue about.

Some are, however, understood somewhat better. One such feature of various Nokia phones is that they are easily adapted to be turned on remotely without alerting anyone. These models are still being sold in various shops specializing in surveillance equipment, and have the advantage of been very common. They are generally sold along the lines of people leaving meetings to go to the toilet, leaving their phone behind in the room. They ring the phone remotely, it turns on and the phone owner can hear what is being said in the room. It is not a great leap from there to getting someone else's phone and turning it on remotely to hear what is being said nearby.

As phone software develops it becomes increasingly open to being hacked in much the same way as computers. Software technologies exist which can scan phones in a room and identify their various makes/models. With this information, carefully tailored signals can be sent to particular phones, prompting the owner to apply security patches, updates, etc, but which actually install malicious software ["malware"] instead, thus putting the phone under the control of a third party. A simple bit of malware is one that monitors the phone's address book, providing the interloper with its details and then notify when it has been updated. For ordinary mobile phones with basic functions, this is not a significant problem; for more sophisticated phones that permit access to emails and internet it is a much greater risk.

Different phones offer other features which can be used against the campaigner – a good example is GPS systems which allow accurate positioning of phones and thus their users/owners.

The software poses other simple hacks for unsuspecting users, which again depend on networks and models. In a recent case a UK reporter was able to access the messaging services of the mobiles of various prominent people because they had not changed the default passwords on their phones.

14.2 Making a phone call

The mobile phone network is actually a series of phone masts and various exchanges dotted around the country. Each phone mast is at the heart of a 'cell', a space that it serves. For a phone to receive a message or call it needs to let a mast know that it is in its cell. It will send out a broadcast signal and select the strongest reply as the nearest mast to communicate with. This location is logged so when there is a message or phone call for that number, the network can route it directly to you. A mobile phone on your car's dashboard may cause your radio speakers to emit a hissing sound as it sends it's location to nearby masts as it changes from one cell to another.

Locating a phone in a particular cell gives the network a rough geographical location of the phone's position. If there are several masts in an area and they all pick up a signal from a mobile phone, then triangulation techniques can be used to pinpoint the location of the mobile phone more accurately. The higher the density of masts the easier it becomes, so in a city this technique is far more accurate than in the countryside.

A good place to make locating the phone more difficulty is on a motorway were the cells tend to be in long lines which makes triangulation difficult. Another place which confuses the system is to be directly underneath a phone mast which also confuses the process by removing helpful data from other masts.

This exchange of communication is going on all the time and is what turns a mobile phone into a tracking device. In the UK all these exchanges are being logged by the various networks at the request of the government and by law. In the US, "enhanced 911" features are required by law to allow emergency services to trace the location of a mobile phone, though of course this is open to abuse by others.

This feature is being turned into a commercial application. There are firms which actively track mobile phones of employees on behalf of their bosses to ensure the employees are where they say they are. It is also marketed to parents as location devices for their children. In theory this is done with the consent of the phone holder/owner as they have to send back a text acknowledging the service. However, this is simple enough to circumvent if they are not in possession of the phone for the length of time required for consent. See the following website for an account of a reporter successfully doing this to a friend: http://news.bbc.co.uk/1/hi/programmes/click_online/4747142.stm. Examples of companies offering this service are www.world-tracker.com, www.verilocation.com and www.tracemobile.com.

There are more and more development on this front as corporations latch onto the mobile phoen as a tracking devlice, so it ceases to be just the state who are doing the monitoring. One company has set up a service allowing people to know the whereabouts of their friends (see http://uk.news.yahoo.com/itn/20080603/tuk-sniffing-out-your-mates-dba1618.html) which also has obvious implications from a security point of view. Another is allowing shopping malls to track the patterns of those shopping in it; though they claim they cannot tell who owns the phone, it would not be difficult to match the data up with CCTV footage to get an image to go along with it (http://www.theregister.co.uk/2008/05/20/tracking_phones/).

Some companies are now offering services which allow you to specifically listen in to other peoples phones, for example www.flexispy.com though some access to the phone in question, as with tracking techniques, are needed to do this. It is, however, a case of how easy latter generation phones can be turned against their users.

However, location is not the only information being logged by the networks; with each phone call they will be recording the SIM and IMEI numbers associated with the phone, the phone's make & model, the location triad, time and duration of the call, the phone number called, and the contents of any text messages. If there are any other features enabled, such as address book back-ups, then they are also recorded.

UK legislation, in particular the 2001 Anti-Terrorism, Crime and Security Act, demands that networks keep logs of various bits of this information. Time, duration and numbers called are kept anyway for billing purposes (BT keeps all such information for 6 years); texts are kept for 6 months (and in the UK are admissible in court whereas actual phone calls are not) and URLs for 4 days. The particulars of other information to be stored are currently under negotiation with the various companies involved. Of course all such stored information is open to the police and other security services to access. The EU is also looking at bringing in similar legislation, though there are data retention issues. In the USA, there is no data retention issue and corporations can keep information for as long as they like, and often do.

As with landlines, the technology to listen in to mobile phones is readily available to the state, and governments are increasingly tapping activists in countries as well other than their own. In the UK and elsewhere the networks have implemented various protocols in their systems that actively facilitate government agencies to listen in on phonecalls. The basic advice is to treat

mobile phones with all the circumspection you would landlines. You wouldn't say anything incriminating over your home or office phone, so don't start doing it with mobiles either.

There is another threat with mobile phones, albeit rarer. It is possible to step in between a phone and a mast by using an appropriately set up computer as a relaying station, which emulates being a mast. If it is close enough to the target mobile phone, the phone will route its communications with the network through it without realizing anything is amiss. The person in control of the router then has access to everything been sent, including the conversation and numbers. This means that agencies other than the state can also tap mobile phones if so desire.

14.3 Network analysis

There is a third class of risk associated with mobile phones and that is analysis of patterns associated with their use. This can be done to a limited extent with land lines, such as whom do you phone the most and when, but with mobile phones there is a greater scope due to the changing geographical factor. In particular, this allows a phone to be associated with a household or individual, even if that phone has been registered as pay-as-you-go. Other information such analysis will provide includes the particular network of contacts associated with that phone and thus it's owner.

Once a phone is used it hooks into the network. So if you use your new mobile to call the land line or mobile of a known activist, your phone is marked for attention. The more it is used in such a fashion the more that phone is compromised and linked into the network. Thus once the phone is used in this fashion then it should be considered compromised, even if you've taken care not to have your name associated with it.

Where and when phones are turned off is also telling. If everyone goes to a meeting place then turns off their phone that is a clear signal that something is up in that area. Likewise, if one person is being tracked to a meeting place, those monitoring them can see if other phones in that cell are switched off at the same time, thus giving them insight into the potential network of individuals associated with their target. Similarly at a meeting, knowing the phones there can be use identify the individuals present. It does not even have to be a meeting – it can be the fact that you've visited someone's house so making a connection between the two of you.

From another angle, if a selection of known phones appears in the same cell or nearby cells and then get turned off it is an indication that something is taking place.

The best solution if you don't want to be associated with a meeting is to leave your phones at home (switched on), or turn them off some time before you get to the designated area.

14.4 Mobile phones and activism

The above sounds somewhat frightening, and it is meant to be. In our view, mobiles phones pose a considerable risk and facilitate state monitoring of us. They are also a nuisance to watch out for. It is easy for someone to slip into a public meeting and use their mobile as a recording device or for taking photographs. This is on top of the sheer nuisance value of people's phones ringing during meetings and people actually answering them. If someone took out a microphone and video camera, we would not hesitate to challenge them: there is no reason to treat mobile phones any differently when they supply the same functions. People come up with all sorts of excuses not to be separated from their mobiles, such as denying the threat, or saying they're expecting important calls, but we've survived well enough without them, so we can do so again for several hours.

As with all security, one has to analyze the risk - but when the executives of large corporations are wary of them for security reasons then we should treat them with the same caution.

To help defeat the various risks associated with network analysis change your phone number and phone on a regular basis. Purchase pay-as-you-go phones in a secure manner (see below), and avoid registering them in your name. Governments are in the process of trying to phase out pay-as-you-go phones so all mobile phones will be registered to individuals. If your country requires a phone to be registered, consider using addresses of friends/squats and false names; swap phones with friends on a regular basis as well.

If you are arrested with a phone you can be sure of two things – the police will forever associate that number with you and they will go through the information on it, including text messages, recent made/received calls, and address book. Calls made during the time of the action will clearly place other phones in the picture and if the police can put names to those holding those other phones then it puts them in the firing line as well. Thus if an action is going wrong, get rid of your phones as soon as possible, preferably securely. What you should not do is ring a land line to say that you are in trouble. Better to wipe free of fingerprints and dump it first.

14.4.1 Meetings

Depending on your required security we recommend the following list of action to be taken, graded in terms of increasing risk

a) Turn off all phones.

b) Place in a box in another room.
c) Remove batteries.
d) Turn off before well before getting to the meeting place.
e) Leave at home altogether.
f) Give to someone else to take elsewhere.

14.4.2 Covert Action

For all our negative opinion on phones, we do accept that they play a valuable role in activism in terms of keeping disparate groups in contact or for use on actions.

The trick is to create a network of phones that are not linked into any other networks. This is known as "closed network" and has been used very effectively by different groups of activists. If the risk associated with being caught is great then it is worth investing in a set of phones to create a closed network solely for that action and following the guidelines set out below.

j.10). Follow the guidelines for purchasing mobiles securely

j.11). Ensure that none of the phones in the network are used to ring any of your friends or contacts, or indeed any phone outside of the network. Once this happens the network should be considered compromised and the phones disposed of (sold on/trashed).

j.12). Keep the battery out when the phone is not required for use.

j.13). Keep the SIM card out when the phone is stored, preferably in a separate place from the rest of the phone; important in case there is a raid.

j.14). Never turn the phone on in your house, office or regular meeting places as it will immediately be associated with that place, especially if it is the first location turned on in. If you suspect your car is under surveillance then avoid using the phone in or near it.

j.15). Avoid patterns of phone use – for example always using the same area and/or time to make the phone calls.

j.16). When making phone calls avoid areas where there is CCTV; consider a bike ride into the countryside, etc, or finding an enclosed bus-shelter.

j.17). Avoid spending longer than 30 minutes in one area when using the phone. Make use of the fact that the phone allows you to be mobile.

j.18). Don't hesitate to get rid of a mobile if it is starting to come too hot. If a phone has been a central point of contact during a campaign or a period of action, get rid of it at the end.

j.19). Consider using your personal phones as a potential alibi – get friends to use them at your home, etc, so creating the illusion that you were using them at the time.

There are many reasons why you might want to make anonymous phone calls to people, both allies and targets. Follow the above guidelines to keep yourself safe from being traced back. If you are targeting someone, don't respond to any calls they make back to you, as tempting as it is to hear their reaction.

A common tactic, which is also relatively cheap, is to ring a number, allow the bell to ring once and ring off, repeating endlessly. Using repeat dial this can be done for some time, effectively blocking the other person's phone line without having to pay for the costs of the call. However, this form of phone blockading may actually be illegal as it could be considered to amount to harassment.

As IMEI numbers are now associated with phone calls, it is no longer sufficient to remove the SIM card to hide your trace. It is important now to get rid of the phone itself as well. When getting ride of a phone that poses a security risk to be caught with, it is recommended the SIM card is removed and melted, and phone itself is thoroughly destroyed. Phone with less of a risk can be sold on the second hand market, though it is preferable to separate out the SIM card and sell it separately.

14.4.1 Taking out batteries and SIM cards

This is often considered controversial because people do not understand why they are doing it. It is a way of disabling the phone so it cannot be listened in on remotely. In the US it has been established that it is possible to monitor a mobile phone even when it is turned off. See for example this news story: http://youtube.com/watch?v=0G1fNjK9SXg

The way around this is to take the battery out, which cuts the power to the microphone and transmitting devices intrinsic to the phone which they are using to listen in. A problem with this is that there maybe secondary batteries in some phones, buried inside the hardware which can also be used and pose a similar risk. It may not be as large, but it is still a risk. Hence, the best advice is to have the phones off and away from you when having sensitive conversations.

Taking out SIM cards does not appear to be particularly effective from this point of view, as the hardware has the IMEI numbers to identify it so allowing those monitoring to zero in on the phone. However, saying that, it will make it harder depending on if they are using the mobile phone networks to facilitate their spying as it is the code on the SIM cardwhich allows the phone to negotiate the networks.

14.5 Purchasing mobiles anonymously

To ensure anonymity take the following precautions when buying a mobile phone:

- Make your purchase in a shop away from where you live.
- Try if possible to avoid town centres where there is a greater likelihood that you will be on CCTV. Many small or second hand shops do not have cameras and those that do are unlikely to retain tapes for longer than a week if at all. High street shops & supermarkets will keep CCTV footage for much longer. Follow the general guidelines for purchasing equipment (see previous section).
- Do not give real details if asked. Many shops do ask for personal information, but do not require proof of ID. In countries such as the UK this is not actually required as yet, and is done under the guise of marketing or for anti-theft purposes, but you are entitled to refuse. However, in order to draw less attention it is probably better to give false information.
- Go for simple phones without all the extra features now being made available.
- Pay with cash.
- Do not register the phone if you do not have to, or else give fake/alternative details, preferably the same ones you have given the retailer.
- Burn all packaging. Most packaging carries various bar codes that permit a particular phone to be associated with it and thus where it has been sold, etc.

Topping up credit

When setting up the mobile, use pay-as-you-go options where possible; this is a more expensive solution, but is much better for anonymity. As with any purchase, this can be used to link you to the purchase and thus to the phone, so follow the same guidelines for other equipment – avoid CCTV, wear nondescript clothes, baseball caps, etc and pick smaller shops. Use cash to purchase top-up vouchers rather than credit cards / ATM machines to top-up swipe cards. Burn or otherwise securely dispose of any top-up vouchers, etc.

Phone wiping

If you have a question mark over your phone and you suspect someone has installed something on it (as opposed to monitoring you through the networks) then one way around it is to wipe it clean of all software and start again from scratch, or less drastically, reset it to factory settings. This is not a trivial thing to do, and will be different for each phone, though much easier in the case of newer phone types. Details on doing this can often to be found though a Google search.
The following useful website provides the necessary instructions from deleting personal data for different models of phones which should be done before passing them on: http://www.recellular.com/recycling/data_eraser/default.asp

15. Conclusion

Remember, security is about empowering yourself to take action in today's repressive society. If you are not taking action, then your opponents have won. There is no such thing as a foolproof system, and there will be an element of risk to everything you do, but do not be put off by this.

At the end of the day we are all motivated by a desire to change the world for the better and that is something that takes courage to do in the first place. You have already made the important steps, so please take away from this article the knowledge to keep making those steps towards your goal. Be empowered, keep fighting and stay free.
If you don't understand some points or need further help, always ask. It is better to be safe than sorry.
The authors have kept themselves active and free for many years now, so there is no reason why you cannot do the same, without making their mistakes.

16. Final Note, Disclaimer and Contact Details

We have written this article based on personal experience, discussing techniques which have kept us active and out of trouble with the law. It is not perfect, and no doubt there are parts you disagree with, we have got wrong or simply missed out. If you have any constructive criticism or suggestions of techniques to add in, please do not hesitate to get in touch. If we agree, we will include them in the next version.

Nothing in this article should be taken as encouragement to commit illegal acts within the jurisdiction you live in. Some of the things discussed may be illegal in one jurisdiction, but not in others. Everything presented in this article is for informational purposes, and the authors and publishers are at pains to note that people should not break the law, no matter how much an ass it is or it protects the interests of corporations over the interests of the planet and its inhabitants. We accept no liability for the accuracy of the material in this booklet or if you get it wrong. Sorry.

Contact us at handbook@activistsecurity.org. The chances are that we are busy being out on actions or campaigning to reply immediately, but corrections and suggestions are always welcome. Sorry, no phone number.