..::www. ActivistSecurity .org::..

A Practical Security Handbook for Activists and Campaigns (v.2)

1. Introduction

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 repressive backlash. Governments, law enforcement agencies and even corporations all have vested interests in criminalizing, disrupting and suppressing activist groups. We need security to ensure we succeed. You 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 hiding most are those in power. As long as governments and their supporting apparatus permit corruption through their closed and secretive natures then we should respond in kind for our own protection.

We also have situations were media organisations with their own agenda will attempt to target campaign groups. Threats do not just come from the state; private investigators and media also need to be factored in as they have distinct issues which also need to be dealt with to ensure your message successfully gets to the public without being intercepted or disrupted by your opponents.

1.3 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 about security that apply to all situations.

Security is a *process* that allows 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 helps keep everyone safe.

A common mistake is to equate security with paranoia. Paranoia is more often used as an excuse not to take action through fear of what can go wrong – normally by over-estimating the omnipotence of their opponents. In our experience truly paranoid people have nothing to fear as they have frightened themselves out of doing anything that would actually put them at risk. Indeed, few even have security measures put in place. This sort of fear effectively means you defeat yourself.

There is no such thing as a 100% failsafe 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 do not put down and pick up security at whim. For security to be truly effective and worth the time and effort put into it, it has to be built into your life. Ideally, it should become second nature to you; that is, you automatically go through the motions that keep you secure. This enables you to have a mindset that helps you avoid errors of judgment 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; or 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. This makes protecting yourself much easier and means you are far 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.

1.2 Setting up the 'Security Process'

Above we noted 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.

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 is 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 adopted 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, and even infighting. They also have poor understanding about how activist groups work, and just because one part of the apparatus 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 of the apparatus.

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 by having a higher level of security than the actually need. This has the advantage that it makes it much harder for them to be penetrated, and any mistakes which do 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 own hype. It is a common trick to send out disinformation about the technological and resources available to be used against activists. 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 everyone. 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 the state, etc like to build up pictures 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 can be easily uncovered through simple things as who is phoning who.

Fortunately for them, 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 the most careful. It is a fact of life, especially when you are 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 shut 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 mistake; 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 pointed out.

Finally, sit down and take time to plan your security out and how it will impact on your life and your actions. Besides a willingness to take the time and effort to achieve good security, the other key feature is good planning. 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.

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 giving them ammunition for smear campaigns and disruption.

When thinking about what security processes you need in place for your campaign, draw up a list of all the 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. However, most of the techniques to deal with the various threats are complementary.

That the principle threat is often 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 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. Remember, security is not just about protecting your people or information, but also the campaign's reputation as that is also targeted – after all there is no point in trying 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 demands are not going to comply fully with their security requests. Your activists 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 make sure that any 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. It is best to have an experienced person dedicated the role of 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.

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.

   Press releases can be treated the same way. Indeed you can sow disinformation by using false names and false positions.

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

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.

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.

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.

   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 rightwingers with a history of fitting up activists.

   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 any other media company 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 the British Monomarks service who have strict conditions on protecting their customers' privacy.

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.

   a. When answering the phone give the group name as oppose to you personal name.
   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 another name.
   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.
   d. Ideally, though it can get confusing, consider using different names for different functions, eg merchandizing, webmasters, etc.

   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

   a. You are just a secretary so do not have access to that information
   b. The information is not to hand and you will have to go to another room
   c. The relevant person with the knowledge is not currently around.
   d. 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. 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, will never ask for the details straight out. 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.

f) ***Need to know.*** Where possible 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.

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

    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).

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

    c. Do you need 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 your office, 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:

    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.

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

2.2 Advanced campaign security

So you are under active surveillance, there are many ways they can gather info about you, so here 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 – even old toner cartridges and anything with handwriting or fingerprints on it. Rubbish bins are a mine of information for the investigator.

When burning paper, do so until it is white and then scatter the ashes. A trick to create a way of burning stuff in most weathers 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.

b) ***Paper trails***; watch out for leaving paper trails regarding ordering your literature. 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 don't use your phones, personal mobiles or campaign address if possible. Collect in person and pay in cash (which may get you discounts as well).

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.

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 information such as this backed up and keep your back up somewhere safe. We suggest in the house of someone with no otherwise 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. These markings need to be checked periodically or there is no point doing this in the first place. Do it in a large cross mark that also marks 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. 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 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, 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.

h) ***Your communications*** may be tapped, and not just by the state. Don't say anything on the phone 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.

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.

2.3 Meetings (Basic)

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

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.

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.

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.

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.

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)

a) 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.

b) 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.

   Watch out for out of place clothes or behaviour. 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.

c) Vary the meeting place each time.

d) 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.

e) 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.

f) 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.

g) 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) 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).

i) Turn off all phones and take the batteries out even before arriving at the meeting site.

j) 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.

k) 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.

l) 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.

m) 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 a 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.
- 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. Do only from internet cafes.

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

2.6 Gossiping

Something very hard not to do, especially when internal divisions arise, but negative feelings are something that can be used by infiltrators and others listening in to sow dissent, or even turn people into grasses with taped conversations. 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.

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 accounts 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.

New people

The first thing to do is to make sure. You will do more long term damage is when people come in and ask questions because they are not clued into the security culture and everyone else immediately jumps into paranoid mode and suspects them to be spies. Explain to them first! We were all young, naïve and eager to take action once, so think back to what it was like then. Later we will discuss about bringing people in gradually and getting them clued in.

If they still do not get it, then you get a bit more worried. 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 theiri parents. 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.

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 undercover actions against campaign groups.

There are ways and means to identify people you suspect, but we suggest you approach an organisation that has 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 are 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.

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

III. 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, maybe in an underhand, divisive way.

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

V. 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.

VI. 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.

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

VIII. 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.

IX. 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.

X. 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.

XI. Boast about their background in other movements which you know is dubious.

(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 is proof that you have an infiltrator on their own. 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.

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 doing 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 advice as practical advice.

II. Put processes in place to protect sensitive material you have or actions you are planning; often if you shut down the information supply they have been accessing they soon drop out anyway.

III. Put together a file of all question marks, with evidence where possible. This should include accounts of suspicious events/statements. You need to record dates, time, places, people present, and 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. 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.

    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 consider third parties and ask them to keep quiet.

    Some ways to actively check our their claims is by ringing their 'work', or following them. A giveaway is 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.

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 peoples 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. This 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.

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.

VII. If you suspect your infiltrator is also acting as 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 tape 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.

What is important is that you do not go public on insufficient evidence – what happens if you've got 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.

Exposing the infiltrator

When you have gathered what you feel is sufficient evidence, you need to act on it. How you do this will depend on the horizontal/vertical nature of your group. For non-hierarchical and 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 then the evidence is 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 before hand, 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 the 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 other 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. Again approach 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 group members with the information to back your claims up.

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.

Dealing with the fallout

Once the infiltrator has been exposed you may want to do one of the following:

I. Consider going to the press to highlight the issue.

II. 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 them as infiltrators. Send a letter to all the groups you are connected with an explanation and what you are planning to do to minimize the problem.

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 greatly in the future. The danger you face here is rumours being spread unchecked.

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

IV. Put in to place processes to minimise the damage to your group, This is important to stope any unnecessary paranoia and in fighting 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.

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

Gatherings

These pose a different set of problems. However, finally authority normally rests with the organisers to chuck them out. 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.

Ask the following questions about them:

- 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 about their clothes, watches and shoes (eg leather at an animal rights event)?
- How did they arrive, and who with? Have they walked, actually leaving 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

Once identified, march them out of the venue.

Grasses after arrest

Particularly unpleasant but it does happen that someone cracks or turns under police pressure/persuasion. It is not always used directly against you but there are signs you can watch out for. 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.

When people start grassing in this 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.

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.

Other evidence that someone has turned is the quality of treatment they get when arrested, for example, one grass got 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 is to 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 ring the office of the newspaper/TV/radio station they claim to work for to check they are genuine. 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. Phone 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, so pass on only need-to-know material.

4. Security for Actions

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

By actions we are covering a wide variety of events and deeds. Not all our tips will be applicable to every type, but we hope that what is and what is not is fairly 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

How you approach potentials needs to be done right. 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.

If you ask them about doing an action and they initially say no but ask you 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, and about being silent.

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.

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 their behaviour as well as words, eg don’t arrange or hint at meetings in front of those not involved which is quite disheartening.

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. 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 the action happening they will accept this.

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. When introducing people into your affinity group note their ability to keep secrets as they become involved more deeply.

4.1.5 High profile people

Some people are naturally under a lot of attention, whether police or otherwise. This maybe because of their organisational role or simply their history of being caught. 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 to back you if things do go wrong, or can be relied on to do their part to make sure that things do not go wrong in the first place.

For example, drug users and heavy drinkers are a liability, as are people with money-draining habits such as gambling. They are much easier to turn or trick into talking, as well as being unreliable. Their need to consume may also cause them to fail to carry out important tasks, etc properly and lie to cover up their mistakes. 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 people with mental health issues where the stress of taking risks may prove too much for them, or that later on, after the action, they may not fully understand the need for security matters.

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.

4.1.7 Security and your affinity group

The final point when bringing your team or affinity group together like this is to ensure that you are all working to the same standards. Differing standards can 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 acting appropriately. Such discussions are also a good way to spot people who are only giving lip-sync to the requests or being too blaise 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 the run-throughs 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 bring along things they shouldn't, 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 affect people. Likewise, if you have made a mistake, it is important that you own up to it, even if it jeopardises everything, that allow your group to go through with an action which may

have been compromised. Also, if it becomes clear that you were the one responsible for the security breach and didn't let people know then people may no longer feel able to trust you.

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, try not to look out of place. Dress appropriately, smart if necessary or a barbour jacket and boots in the country, and depending on the area, maybe have a cover story - A good one for the countryside is to bring a dog lead with you and say you're dog has run off. Basically the more natural you act the better – and don't be rude to people.

Plan any surveillance carefully, and watch out for 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. 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. Don't forget to use counter-surveillance techniques to ensure you are not compromising yourself and your fellow activists.

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. Know your access points in and out and make sure your drivers are familiar with them. Have back-up rendezvous points should you be forced to scatter.

Some useful techniques is to:

a. Go out in male-female pairs so you can act as a courting couple if necessary.
b. Bring a dog lead and pretend your dog has legged it and you are looking for them.

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 rendezvous 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.

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, or extra paranoid or suddenly changing pattern. The chances are that these will bring more attention to you. Act as naturally as possible, as if there was nothing untoward about to happen, or has happened. Discretion is much better than being paranoid. Have cover stories 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 have changes in phone call patterns in the run up to or immediately after an action to particular individuals. Indeed, the less connections that can be drawn between the individual parties the better.

4.4 Communications

Meeting to discuss and plan – most of what was said under campaigns 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 do not use obscure half broken sentences. The best approach is to arrange to meet people and pass the message on verbally, or write it on a piece of paper to show them and burning it immediately afterwards.

Arrange meeting by face-to-face meeting if possible; don't simply turn up and have a meeting there and then. The less that needs to be said at the initial invitation the better. If someone is going 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 doing anything in your social group as it will rapidly become obvious to those not involved that something is up.

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 and don't park any hired ones near your house. Where possible avoid using credit cards, though it is hard to hire vehicles without one these days.

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 link you to the equipment and are not necessary. 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 not a good idea. Make purchases as soon as possible, and not the day before the action – the longer the gap between purchase and action the better.

Purchase in advance as much as is possible – doing it the day before is a big risk. The longer the gap the less likely shopkeepers are going to remember your face or CCTV footage will be kept. 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 the materials to where it is to be stored, carry it wrapped up so it cant 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 if it going to stand out.

Stuff for the action should be cleaned of fingerprints using white spirits or washing up liquid.

4.6 Clothing & other tracables

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

These leave distinctive marks, and cuts and wearing in the tread 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: Watch out for getting mud on the rest of your clothes, especially your trousers.

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: impressions of footprints can now be taken at the roadside by the police.
Glass is another telltale sign on shoes and traces can be matched with broken windows.

4.6.2 Clothes
Depends considerably on the action. Non-descript 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 – camoflage 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.

III. Zips are also noisy and buttons should be preferred.

IV. Make sure you have nothing reflective on you.

V. If doing an action in town or where you are likely to 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 giveaway. Snoods are good as they can be quite obscuring, and they are a legitimate clothing item. Ski-masks are not good as they give away too many 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.

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 alternative of providing the forensics team with no information at all is to provide them with too much information by deliberate contamination. The same goes for gloves as DNA can now be extracted from the inside of hats and gloves.

4.6.4 Fingerprints
Wear gloves, though some of the latex ones do 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 ready in a bag and soaked in white spirit.

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 pretty convincing evidence. Markings can be as simple as a lot of fingerprints over the relevant spots.

Techniques to use with maps are

c. Do use markings, even pencils
d. Use laminated maps which can be wiped of tell-tale marks quickly and don't have as big an issue with fingerprints as paper.
e. 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 – use an internet café to do this.

4.6.6 Other materials
It is good policy that before you leave to go on the action, you remove any unnecessary items from your clothes. 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 a full key ring. Bring some money for phones though.

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

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

a. Use plastic covers on the seats.
b. Put down newspapers
c. Have cleaning materials ready in advance, especially for transit vans. This includes black bin bags for disposing of the newspapers, etc.

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, and ruin any alibi 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 something often forgotten about, but is quite crucial as to whether you actually get away with your action or not.

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. If in doubt take the more cautious option.

Souvenirs of an action are really not a good move. 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. Make sure you budget time for this.

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

Boltcutters etc may have telltale 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, have the material bought in advance and don't wait until after the action.

If you are leaving with equipment people in the vehicle can help by filing down telltale marks, wiping stuff clean and general helping with the disposal process. Before you set off, include the clean up material in the check-list – eg, cloths soaked in white spirit, filing tools, working lighters, bin bags & cleaning agents, etc.

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.

A good few 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 Communiques & Photos
Make sure you can send these securely; if it will compromise you, then don't send. Consider waiting a while so the heat drops down. Never do from your home or hometown – the greater the distance the better, and avoid CCTV as much as possible.

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 below 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 that have 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 prepares them. It is advantageous to put the set of numbers on each phone for speed-dialing purposes.

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. If making a series of phone calls rotate them around phone boxes – never stick to one or two - but not in a pattern you repeat.

5. 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 phonebox), put not at the expense of making you stand out to passers-by.

6. 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.

7. Use 141 in front of numbers (UK) only. 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 of guaranteeing security but of adding an extra layer of security.

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

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

4.10 CCTV

CCTV is everywhere these days, but not impossible to hide from. Learn to recognise, but be aware that they can be in shops but videoing what passes the windows. *Avoid looking up*; baseball caps are good. Quality does vary considerably and some do have sound or night vision.

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

4.11 Travelling

When driving, pick country roads and motorways, avoiding towns as much as possible as that is where the greatest concentration of camera are found. Keep within the speed limit, so as 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 it off until it was time to travel again.

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 you should consider if you should be on the roads at all as you are then more likely to be stopped in spot checks.

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. It is best to have two people in the front, looking smart, ideally a man and a woman, with everyone else lying down in the back.

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.

4.13 Being chased
It may happen that you pick up a tail while leaving a covert action. Depending on the action, you may either decide to accept the fact. However, if the situation is a serious one, it may be worth trying to lose it

4.13.1 On foot
Scatter in groups of between two and three, preferably matched up to speed, but in groups of no more. Solidarity is all very nice, but there is no point all getting caught.

Move in different directions. Always have a secondary rendezvous and time in case this is necessary. If this is a possibility, people should have maps of the area (no markings) and be familiar with where they are and what they are looking for.

Hiding may require you to keep your cool especially when there is someone standing quite literally over you, but the key is to relax and keep control of your imagination. Gardens, woods and hedgerows are all good for ducking into.

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 the passengers get caught later they may need to justify why they tried to evade capture in court.

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 so many rings means trouble, but that they do not answer it. 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.

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 otherwise, 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 DVLA). 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 people have suggested using false number plates which will confuse cameras and also throw investigators trying to trace the car, however, modifying number plates in anyway (including putting mud on them, or using tape to create new letters) is illegal. 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. 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 demos 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 outside of your house to be watching you, though some are to be found in the houses of neighbours.

4.15 Debriefing

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

a. Go through what went right and wrong so you learn from mistakes and improve for future actions.
b. With what went wrong, consider where are people now at risk and what can be done. However, it is not reasonable to expect everyone to take the fall in solidarity with one person.
c. 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 part of human nature. A debrief gives people a chance to get this off their chest so making it less likely for them to talk to others. If someone needs to talk further they should not do it with anyone not involved in the action.
d. Remaining responsibilities to deal with should have already been planned for, but if there are new unforeseen circumstances that have cropped up they may have to be dealt with.

4.16 Shitting in you 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 such like.

On another level, it refers to actions with significant consequences and which may even lead to raids. Action with these sort 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 hardline 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 the further away from you & your town 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 find what applies to you and your action. 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 any investigator 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…

This list is far from comprehensive, and there will be things we will have missed or only briefly touched on. If you think we have got something wrong, or missed out some useful information, let us know.

5. Security for Demonstrations

If you are a person involved in covert activity you need to strongly 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 not point having 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 demos of all types:

- Avoid calling out peoples names; use pre-arranged nicknames or generic shouts.
- 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.
- Never, discuss plans at a protest, even meetings. Demonstrations sound noisy, but directional microphones can easily pick up conversations – including from helicopters.
- Masks can now be confiscated under Section 60AA, however, that does not make them illegal; however, the police are just as likely to say that your are attempting to be intimidating and harassing by wearing one. Baseball hats and coats with high collars can also be used to hide the face, as can placing banners in front of you.
- 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.
- Avoid carrying ID, though if you get arrested and cannot confirm your identity then they may use this to keep you in the police station for longer.
- 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.

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. 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. Likewise, consider if putting up posters on your car windows will be drawing unnecessary attention to it, especially if they are left up on the windows when the car is parked up.

Try to avoid going to and leaving a demonstration by oneself.

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. 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.

5.5 First Aid
The state and other opponents will often 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 will not be able to help others.

Self-defence training will also teach you how to take and/or deflect blows so they do not do as much damage. Another use of first aid is how to deal with tear/cs gas.

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 the 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 demos, 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 in the situation. 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 make 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 truly 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, 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

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 and can draw more attention to you.

Knowing that your under surveillance or that your house may be bugged may have its 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. As, 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 rationally, quite often the information is 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, the 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 aside will have to be put aside for the practical reality. Your aim is to get away and continue being active, not bringing attention to yourself.

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 asked to be a grass – see the article on www.activistsecurity.org for more on this.

6.2 At Home

Below are some techniques and advice for protecting yourself at home. A rule of thumb here 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 go, and change each time. Leaving mobile phones in the house, of course.

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. Considering avoiding having samples of your handwriting around.

Have a process where you do not leave stuff such as envelopes, notes, etc lying around, where a grass who has got close to you can read or pilfer.

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 cistrines, 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 what it is stored on it.

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

6.2.1.1 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, then any panicky action will be noted and thus you will bring 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 point other people out to them as being worthy of attention.

So, 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 a bit 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 it was particularly good they wouldn't be stopping by to see you for a friendly chat, but dragging you down to the nearest 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 actions and being very effective to.

6.2.2 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 acting to make you paranoid. 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 it would put you, others or your plans in jeopardy for your opponents to hear.

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.

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. Use of appropriate codes works, though in our experience, they will sometimes check up these cover stories. For example, one activist was followed out of the country to a family funeral because the state thought the funeral was an excuse for something else. The best advice is to avoid planning stuff over the phone and email, unless the email is encrypted.

Some activists recommend using a programme called Skype, if you have broadband, to make phone calls, which allow them to be made via the internet. Its usefulness here is that you do not have a phone bill listing the people you have been calling. However, one must be aware 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 more risky.

For email, use PGP encryption for everything. The more people who use it the better. See elsewhere for a fuller description of email security.

Remember, the phone and email are useful for facilitating and initiating stuff, but they do have their limitations.

The phone can also be used as a listening device, so take care talking around them, whether landlines or mobiles. And remember, you never know what your guests are carrying, as some activists found out when targeted by undercover reporters. Finally, whispering on the phone does not work.

6.2.3 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 through using special sprays. A useful way around some this of this is to use birthday cards and the like.

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, and see the guide to writing letters anonymously for more information on that issue at www.activistsecurity.org

6.2.4 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 however an uncomfortable feeling, but one activists may 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. Saying that, if your lock suddenly gets very stiff as if the mechanism is dodgy, it could be the sign of a hamfisted lock picking attempt.

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 it's 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.

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

6.2.5 Being bugged

Police (and private investigators), either through covert intrusion or during a raid, will and 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 – most are there to pick up on voices. Old tricks such as running water and having loud music on in the background are not going to be that effective against them.

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 does 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.

6.2.5.1 Scanners

Scanners are simple devices that pick up on radio frequency transmissions; they can be bought in shops (eg 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.

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.

6.2.5.2 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.

6.2.5.3 High Tech Surveillance Equipment
Even if you are sure that you are not being bugged, your enemy 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 been subjected to this, though we have heard that he 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 who they are and where they live. Be friendly with them. You don't have to tell them you are politically active, though in some cases it can actually be an advantage.

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. It is unlikely, but it has been known to happen in a couple of cases, but one where heavy surveillance was expected.

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 cant get results from bugging and monitoring your home then they will not keep it up forever, or cut back on the time and effort they 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 wanting to check 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 note the car 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 load of maps in it?
- Has the details of the garage on the back windscreen been taken off?
- 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.

6.4 Your car

Your car is a very useful way of tracing back to you, and building up a spurious picture of your activity, especially if the car is used for group activity. A useful technique for minimising this is to register it to a PO Box and change the registered owner/keeper regularly. You can do this as often as you want.

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 course will teach you what you need to know

7. Being tailed

We have made a note on how to spot a tail waiting to pick you up at your house in the previous section, however when out and about it is also possible to pick up tails.

If you followed by professionals it will be very hard to tell. If you are the target of a major operation then they will throw far more resources your way. It is rare for them to use just one car. In one operation 14 different vehicles were used to follow an activist's car up a motorway. The problem is that as you lose one tail, another coming from a different will simply pick where the first one left off – even easier where you are following a pattern

However, in standard surveillance of activists they have fewer resources available than is ideal so tails can be spotted with some of the tricks below.

Suspicions of seeing the same face or car before is not evidence enough of a tail – you have to be really sure; only when stuff repeatedly occurs can you start to build the picture up. We will not cover tailing techniques here – these can be readily found on the internet, other than to say that most tailing will involve a team of people so faces, like vehicles will continually appear and disappear. More important for activists is that they are observant and forcing tails to expose themselves, so that they are able single out faces and vehicles to watch closer. Remembering faces can be difficult so try to single out sets of features rather than whole faces.

If you suspect you are under surveillance you can attempt either to lose them or confirm it. For activists, we suggest that you focus on confirming so you can act accordingly. The problem with losing a professional or a group of tails where you do not know how many there are involved, so you could be picked up again later on by others in the team you've not identified. It is always important to 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.

Another situation 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 of further attention. This is why counter surveillance 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 better you get.

Sometimes it is worth erring on the side of discretion. Remember, most activists will come under surveillance at some stage, as the authorities want to build up a profile on them, so it is not worth encouraging further attention if it can be helped.

7.1 Vehicles

If you think you are being tailed, start using routes and techniques that will make it obvious. The following are some techniques to identify and deal with surveillance.

a. Number plates
    - 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, eg 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.
    - 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.

b. Watch for cars with sun-visors down permanently – done to stop faces been seen fully visible.

c. Cars 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.

d. 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.

e. Indicate to take a turning at a junction and then go straight on. Has the suspected tail done likewise; not particularly effective as tails often don't indicated at all because of this.

f. 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. When they have passed spin around and go back. If you don't go back, keep an eye 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 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 can be pretty confident that they are the tail. This technique will work 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 tail to act in a way that gives them away or else lose them.

- Drive into farms 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 routes that is hard for them to pick up on you again, or certainly if they do then they do not have

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

   - Follow you down the cul-de-sac, 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. On a narrow cul-de-sac you can be gone before they have a chance to turn around.

   - Wait on the road outside the cul-de-sac knowing that you are practising 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.

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

i. Be random and vary your routes a lot as a matter of course. Allowing yourself to develop a pattern makes it easier to follow you, as they can wait further along your regular route before they pick you up. Also, suddenly breaking a pattern can be a sign that you are up to something. So if you live on an estate etc, you also need to be monitor potential tails placed at the access points to the estate.

j. Enter a petrol station and see who else stops. Is there a car that is not refilling or simply parks up?

k. 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.

   If you want to lose them, let the tail go on and follow their route out if they've not turned around already. The chances are that they'll be expecting you to go in the opposite direction to the one they are heading. You need to keep your cool on this and maybe pull in to let other cars behind you pass as you do not want to suddenly appear in their rear-view mirror.

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 surveillance has effectively failed.

l. 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 why using your car to go to secure meetings and for covert actions is not a good idea, as the chances are you will not locate the device if it is properly hidden unless you use a proper scanner on the vehicle or given it a thorough check over.

   Saying this, there are ways of testing to see if you have one, if not necessarily guaranteed to work. One is to 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.

7.2 On foot

If you are being followed on foot, they are again likely to use a team of people rather than just one person. They will dress nondescript and have few identifying marks or clothes (other than that standard policemen are generally quite easy to spot even in plain clothes just by their walk and stance).

The average tail is not hard to spot as they do not react well to sudden changes in your action. A professional team, however, is quite difficult to throw. The key to spotting a tail is to either throw them by doing something unexpected or force them into a course of action where they betray themselves. The following techniques will help detect the less competent tails, though remember that a professional will also be ready for these. An advantage most activist have, is that those tailing them often don't expect the activists to be sophisticated or security conscious so they may be less prepared.

a. Don't wear clothes, jewellery or hairstyle that stand out as these simply act as marker for them and means that they can spend more time hiding from you. However, a sudden significant change in appearance by yourself can cause them to give themselves away as they try to check that they have got the right person still.

b. Don't have habitual methods of doing stuff, eg going to a pub, town, etc as this means it is much easier for them to stake out your route as opposed to your house.

c. 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 advantageous to practise watching people in the street on how they window shop and such like.

   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

d. 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.

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 when you are looking for people don't forget to watch those who have passed you by and then stopped.

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

g. Stop at a cinema or theatre and read the boards giving you an excuse to stop and look around.

h. Do people suddenly change direction and cross the road from the other side of you when you do something such as go down an alley or into a shop you do not normally enter.

i. In a bookshop is there anyone looking at the same books as you just browsed through, in particular any political ones?

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. 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.

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. Waiting in a queue for a bus is a good way to spot tails. A way to lose them is to suddenly leave the queue as boarding starts. Maybe let a few buses go by to see who else is waiting – 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). Suddenly 'realising' that a bus across the road is the one you want and making a dash for it is a good way of exposing and/or losing a tail.

n. Some quick ways to loose a tail:

    a) Ring a friend and get them to pick you up from the kerbside in a car.
    b) Dash across a busy road the moment a gap appears and disappear down side streets or into any building with alternative entrances.
    c) 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.

o. Expect them to change glasses/hats/coats etc.

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

7.3 The Check Route

Some experts recommend setting up a 'check route' to detect if you are being followed. This is a several mile walk through town, quiet streets, and other places passing things allowing you to carry out a number of the above surveillance techniques, without necessarily raising suspicion that you are looking for tails. To make this more effective work with other activists where they can wait at prescribed places (and blending in so they are not noticeable) to see if anyone is following you. This can be difficult to set up however, and if those following you have a good idea of what other activists look like then it can be a bit of a give-away. Ways around this are:

a. To have a fellow activist 'accidentally' meet you on the street so you have a reason to stop and monitor the surroundings.

b. To have the others watching you positioned in places where they will not be spotted, such as in cafes.

This sort of counter-surveillance check will take time and effort to set up and you have to be aware that the process of setting it up may also be during at time when you are under surveillance. There is no point having a check route if your tail knows about it.

7.4 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. 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). The problem is that as soon as you start acting unpredictable it confirms their suspicions and encourages them to follow you even closer and for longer.

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

We will not go into much detail on computers here other than to cover the basics. There are a number of sites on the internet which go into computer security and protecting your privacy online in more dept. However, as a bare minimum you should be doing the following:

8.1. Security

I. Install and regularly update anti-virus and firewall software. Free programmes such as AVG (www.grisoft.com) and ZoneAlarm (www.zonealarm.com) are available for Windows. The important feature is that live update is activated so they are continually up-to-date.

II. Install a spyware detector programme such as Ad-Aware which is free from www.lavasoft.de.

III. Deleting a file does not remove it from your hard drive, etc. In order to do this it needs to be properly wiped, using a programme dedicated to doing this. Recommended ones are Clean Disk Security and PGP.

IV. Encrypt any sensitive files on your computer, CDs or floppy disks using a programme such as PGP (or GPG). Ideally, you will stuff all files in to one big archive (eg using WinZip or StuffIt) and encrypt that. This means that even the file names are hidden. Wipe the original files. This should be done every night when you've finished using the computer. Alternatively use disk encryption

V. Chose passwords that are effective – longer than 16 characters, including upper and lower case letters, number and symbols if permitted. Weak passwords are easily broken. Password protected computers are not secure to the prepared infiltrator so encrypting anything sensitive is also needed.

- Passwords should be changed on a regular basis.
- Do not write them down and stick them under your chair or desk – these are the first places that a spy will look.
- Do not base them on the names of family, pets or dates of birth
- Do not simply use dictionary words

VI. Back up your computer in case it is stolen but keep the back-ups secure somewhere else.

VII. Consider switching away from Windows to other operation systems such as Linux or Mac.

VIII. Avoid wireless keyboards as they transmit quite a distance as well as to your computer.

IX. Keep important/sensitve data and PGP keys on removable media such as memory sticks.

There are devices available which can be attached to your computer and will record everything you type, including passwords. The chances are that you will not be able to find them. Likewise, there is equipment that will pick up what you are typing by bouncing a laser off of your window. However, they are unlikely to use these except in major cases. If you suspect that you are going to attract this sort of attention, then you need to strongly reconsider if you should be using your computer at all.

8.2 Internet Privacy

I. Emails are not secure, and very easy to monitor. To keep them private, use PGP encryption (www.pgpi.com). Don't say anything in an email you would not be prepared to justify in court.

   If you want to contact another person without those watching you knowing who it is you are in contact with set up fake email accounts on free webmail sites and use them instead. Consider using it as a maildrop system.

   You can also look into using 'remailers'.

II. Be aware of spam – unsolicited emails, even if they look genuine, such as from a bank. Never buy anything, or even click on the links to websites contained in unsolicited emails. Messages from banks, eBay, PayPal, even warning you that you have a virus are all fakes. If in doubt ask someone who knows about computers, but err on the side of caution.

   If someone sends you an attachment you are not expecting, do not open it, even if you know and trust that person. Email the person, asking if they really did send the attachment to check it is not a virus.

III. Avoid using Outlook or Outlook Express for your emails. Consider using an alternative such as Eudora or Pegasus. Outlook is notoriously buggy and a significant agent of virus transmission.

IV. Avoid using Internet Explorer to surf the internet – use an alternative such as Opera or Mozilla. If you cannot avoid using Internet Explorer, switch off Java and ActiveX.

V. Every time you access the internet you leave a trace that can be used to tie back to you. If visiting a website you don't want people to know you are interested in, use an anonymizer website or an internet café. If you suspect you are being monitored, do not do anything sensitive from your home computer. Watch out for CCTV in internet cafes so pick small, obscure ones.

VI. Avoid using details that can be traced back to you. Use pseudonyms and email addresses with fake details were possible, when posting messages, etc. Do not try to be ironic by using something that ties back to you, even indirectly.

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, email 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 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

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 (RIP) Act

The main issue for campaigners here is that if they seize your computers, then they have the powers to demand you surrender the passwords to your computer and any encryption techniques your are using. Failure to do so in theory can result in a two-year prison sentence.

In practice it is quite unworkable and rarely used, as it is hard for them to prove that you have not actually forgotten it:

- through lapse in time since you last used it;
- it is quite fiendish so hard to remember in the first place;
- from the trauma of the raid when your computers were seized.

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 let 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 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:

    a) Bring it up as a general point at a meeting without particularly naming and shaming. This has the advantage of reminding others of their responsibilities as well.

    b) 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 future 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 and 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.

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, an not necessarily all the police forces. Police forces 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 police forces.

The main changes of relevance to activists are:

- Improved forensics catching traces that would have been missed on materials, etc previously.
- 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).
- 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 ceases 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 that is quite closed. 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 do 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 and outside of any public glare.

13. 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, and stay free to keep fighting.

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.

14. Final Note, Contact Details and Disclaimer

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 info@activistsecurity.org - PGP key available on request.

15. Other Articles

The following two articles, "Using Mobile Phones" and "Writing Letters Secure" are taken from other sources and only slightly modified for inclusion in this booklet.

15.1 Using Mobile Phones

Contents

6. What the law says
7. Future developments

Like them or loathe them, the mobile phone is a defining tool of the modern activist. However the benefits they bring in terms of anonymity and mobility have a flip side, of being yet another tool Big Brother can use to keep an eye on us. When the mobile phone becomes indispensable it is a threat to your security and privacy.

But all is not lost, for with a few simple precautions you can use the mobile to it's full potential at only minor inconvenience and little threat to yourself (other than the occasional nuked brain cell).

15.1.1 The technical bit

Feel free to ignore this, but it will give you a deeper understanding of how mobile phones work and the risks they pose.

Mobile phones come in two parts, the actual phone with screen and buttons, etc; and the "SIM card" that associates the hardware with a telephone number. The SIM card is a small strip of plastic with a gold circle on it. It fits in the back of the mobile, usually behind the battery. Each SIM card is unique and identifiable by the mobile number. Appropriate SIM cards can be swapped around.

Most people are paranoid about the SIM card, but the phone itself is also marked with an IMEI number the "International Mobile Equipment Identity" number.

When you make a phone call both your SIM card and IMEI number is broadcast to the mobile phone network.

What makes a mobile phone quite literally mobile, is the presence of mobile phone masts scattered around the country. When your mobile is turned on it and the network constantly check with each other as to where is the nearest mast for it to communicate. In any one area, there may be several masts, so the network and your phone communicate with them all in order to work out which is the best one for you to use.

This is the nasty bit, for using the information provided by these checks, it is not hard to identify roughly where the phone is located. Some estimates claim that this works down to 10 meters, others make more accurate claims. However, the fact that they can locate you to a particular area is damning enough.

Bring in features such as global positioning services (GPS) as now comes available with most phones, whether advertised or not, then your mobile is essentially a homing beacon for those with the power to access this information. This can amount to circumstantial evidence that will stand up in court when tied in with other facts.

15.1.2 Playing safe with mobile phones

That is the downside of mobiles, but none of it is surmountable and there is plenty of fun to be had. In these days of oppression against activists, the mobile allows you to continue to be active and effective while preserving some of your privacy.

The same warnings regarding landlines being tapped all apply equally to mobile phones. The only difference is that there is not a specific phone to tie you to, and you are not necessarily registered to the number. So, if

you can purchase a phone anonymously and use it with a few simple precautions then there is no reason why those trying to invade your privacy will ever be compromised.

15.1.3 Purchasing mobiles anonymously

To ensure anonymity, the law does not forbid you from doing the following tips when buying a mobile phone.

Purchasing

- 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 few weeks if at all.
- Do not giving your real details if asked. Many shop do ask for your details, but not proof of ID, and you are not under any obligation to inform them.
- Go for simple phones without all the extra features now being made available.
- Only pay by cash.
- Do not register the phone – there is no legal obligation to do so.

Topping up credit
When setting up the mobile, use pay-as-you-go options only; this is a more expensive solution, but required for anonymity.

Unregistered pay-as-you-go phone calls can be paid for either by using top-up vouchers, or by a swipe card inside a shop. We recommend that you only use top-up vouchers purchased in cash. Using a swipe card to top up within a shop leaves a trail of evidence back to the shop where you could be identified by CCTV or eyewitnesses.

15.1.4 Using personal mobiles safely

By personal we mean mobiles that are going to end up being associated with you. The moment you give out your number to friends and associates it will end up on any network of contacts being monitored by the state. If you are an activist, or your associates are activists, then this will immediately compromise the security of the phone.

Never say anything on a personal mobile phone you would not wish to have to justify at any point or may incriminate you in any way. Although the mobile may not be used in an action, it use may point to you as being involved and cause you to be investigated.

Do not take personal mobiles into meetings, and preferably do not even bring them with you. Mobiles are potential listening/tracking devices and should be treated as such.

If you are on your way to a sensitive meeting, turn your mobile off and remove the battery well before you get to the meeting point, or you may be giving the meeting point away. Even if the meeting is not secret, it is best not to have it present, as you never know what else might be said; besides being very bad etiquette, the safety of others may be put at risk.

Personal mobiles should be avoided being brought on actions where possible. If you have to bring them, such as for ‘mobile’ demos or if you get separated, take the batteries out until they are needed.

Another risk area of mobile phones is when people are doing internet activism; there is no point taking a load of security precautions if your mobile phone logs are going to place you as being in the area at the time, or alerting others to the fact that you were in that area so giving them an avenue of investigation.

We currently recommend against purchasing the higher end of the mobile market where phones have built in camera and other gadgets. Again camera phones hold potential threats to your security, and give them a face to match to your voice. It has not been necessary so far for people to see your face when speaking to you, so it should not matter now. From those concerned with privacy and activism, it is another compromise.

Never enable GPS or similar such services on your phone if you can help it. Features such as these appear to make life simpler but contain inherent threats to your security.

SMS / Texting is very useful but also one of the easiest methods to monitor. It is known that scanning software is available for monitoring them, but tends to be only in the hands of security services as opposed to the police. However, if a hacker was to break into a mobile phone operator's databases then the chances are that they too could monitor in what ever fashion all the information passing through, and pick up on sensitive details that you are sending via text. Make sure you delete your text messages and never write anything you would be unable to defend in court.

Finally, mobiles can also be used to confuse. Say one mobile phone was used in an action and you have been accused of using that phone at that time. A possible defence is to say that it could not have been you as if they were to look at the logs of your actual phone, that everyone knows is yours, then it was in a different place altogether. In other words, the tracking capability of mobile phones can also be used to provide alibis, especially if calls were made from the phone at the time of the alleged offence.

15.1.5 Mobile phones and activism

There are two scenarios to consider here. The first is where mobiles are used to facilitate the action, but not the action itself. The second is when the mobile is an intrinsic element of the action.

Facilitating actions
In the first case, this could be when an action needs to be coordinated. If there is a lot of risk attached to this, it is worth investing in a set of mobiles to be used specifically for it. Second hand mobiles may be useful in this case, as the chances are that after the action the mobiles will have to be discarded – just do not buy them of friends! The reason behind this is that if you have a set of mobiles that have never been associated with your network of contacts and friends, it is impossible to connect them back to you.

This means you can set up an anonymous network that will not draw attention from the various authorities listening in. Avoid bringing attention to it by not saying anything explicit on it, but using code. Keep the batteries out of the mobile until they are required, and when testing that all is working fine, chose an area free of CCTV. Testing that the mobiles work and that everyone can use them and has the relevant numbers is important.

We also recommend that you burn the packaging that comes with the phones. The mobiles should be disposed of afterward, ideally by burning. It is no longer enough just to destroy the SIM cards and reuse them.

Mobile phones for activism
As noted, mobile phones are a very useful tool. There are many situations whereby you want to contact another telephone number anonymously. So some guidelines:

I. Follow the above guidelines for purchasing a mobile phone anonymously.
II. Do not ring your friends or contacts from the mobile; if you have to do this, then get rid of the mobile immediately afterwards as it has been compromised.
III. Keep the battery out of the mobile when not in use.
IV. Keep the SIM card out of the mobile when not in use; preferably store them separately in case there are raids.
V. To make the phone call, travel to the area avoiding CCTV as much as possible. A quick bike ride into the countryside or a suburban bus-shelter usually does the trick.
VI. Try to avoid spending longer than 30 minutes in one area. Make use of the fact that the phone allows you to be mobile.
VII. Do not slip into a pattern of using the mobile at a certain time or certain place or it will end up as being little better than using it at home.
VIII. Do not answer calls to the phone and ignore any messages they leave on your answering service; as tempting as it is to hear their reactions, do not play into their hands.

A good deal is made of mobile phones as a tracking device, and this is true. It is based on the strength of signals being exchanged between the mobile and the surrounding masts; mathematical analysis called triangulation is then used to deduce the area where the mobile phone is. In feedback gleaned from police cases this would appear to be more difficult than expected; however there is one known incident where police turned up within half an hour of phone being used. Two tactics for defeating this are

a. Sit directly under a phone mask – supposedly this plays havock with attempts to triangulate
b. Use motorways; masts are placed in a linear line down motorways, which again makes triangulation difficult. Though avoid using your own car!

Depending on how much you use the phone, what you say on it and how your target reacts, you need to consider changing the SIM card after a length of time. The heavier the use, or the more legally risky stuff you say on it (or not as maybe the case) will require regular changes of the SIM card and even of the phone itself.

Targets react to phones in several ways. They can end up blocking that number altogether, in which it will be useless against that target. However, as most people involved in activism have more than one target, it is simply a matter of moving onto the next target that has not blocked it. In many cases, the block may only happen for one number in a company, and not others. As it is likely that it is only the SIM card that has been blocked, you only need to change this in order to be able to contact that telephone number again.

Some companies simply send out a warning that your calls have been logged and the police informed. We know of one situation where police did turn up within the hour, though this appears to be the exception and only followed on after heavy use of the phone in the same area over a few weeks. To play it safe, do not reply to the message, take the battery out at once and leave the area, preferably stashing the phone somewhere on the way. If you have taken all the above precautions, then there is little anyone can do to identify you.

15.1.6 What the law says

Stolen and reprogramming mobiles
Stolen mobile phones can be disabled across all networks as the different operators and the government are now co-operating on this issue. A side effect of this is that phones used as part of activism now also have the potential to be blocked, though we have not been made aware of this having happened. This blocking is

done to the actual phone (through the IMEI number) and not just to the SIM card. For more information on the UK initiative on stolen mobiles see www.immobilise.com.

It is possible to re-programme the IMEI number in a mobile, however this is an offence in the UK with a maximum 5 years imprisonment.

Repeat ringing
Ringing another telephone number constantly may amount to harassment, though it is not clear what the legal situation is regarding allowing it to ring once before canceling the call. This is a tactic thought to be favoured by some activists who do it repeatedly over a length of time for effectiveness. This is not a course of action we recommend as it could be illegal, since it may amount to harassment or an offence under the Telecommunications Act 1984

15.1.7 Future developments

Mobile phone manufactures and software companies are working very closely together to develop new services for mobiles. There is a natural trend to turn to the mobile into a miniature computer. Unfortunately, these come with a lot of security risks.

There have also been a number of stories about commercial systems now being able to use mobile phones and the internet to monitor people. This is being done under the guise of monitoring lazy workers or protecting children. However, the obvious threat to civil liberties is there.

So far, in order for these commercial services to work, a text message is sent to your mobile from the tracking service, and you have to reply (that is give your assent) to activate it. It should be standard policy on your part, never to reply to unsolicited texts or texts from numbers you do not recognize. If you get one from one of these services, then simply ignore it. It only becomes a threat if you reply to it.

The risk is, if your house is broken into by whatever authorities or company are watching you, and they do the reply for you (it would be relatively simple to arrange to have a text message sent at the appropriate time, and subsequently delete it, in which case you would be blissfully unaware). The simple solution is to take the SIM card out when not using it, especially at night, and store it separately, as we have already suggested you do with phones being use for activism.

Note: there is a lot of information on how mobiles can be used to spy on you at http://www.spywareinfo.com/articles/cell_phones/, but note that this is principally for the US situation. How it applies to other countries is not clear.

15.2 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 accounts of how one person writes letters to ensure complete anonymity. Not everything they do is necessary - play it to your own needs and situation.

15.2.1 Writing letters at home

Preparation is everything. It comes in two stages: acquiring the materials, and preparing the writing room.

I tend to purchase my material out of town from well-known shops, buying the most popular brands, in particular generic shop brands. Nothing fancy. Make sure everything is in plastic wrappers so you don't touch them. When you get home, keep them separate and burn the receipt.

At home, I set one room aside for the purpose and give it 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 hovered and the walls dusted. Any animals are kept out.

I then have a shower, and put on freshly washed clothes. Wear long sleeves, and give you hair a good brush, tying it back if necessary.

When writing, I put on a new pair of washing up gloves before I do 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 you want 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 your 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.

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).

15.2.2 Note on using computers & printers

There are a few things to watch out on if going for the printed text option.

A. 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, 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 goes. For more information on this, visit http://www.privacybasics.info/

Finally, if writing something particularly sensitive, then use the free space wipe option on the mentioned software to be on the safe side.

Alternatively, if the environment is safe enough, then use a university or library computer, so there is no connection to your own computer

B. Printing

Printer 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. These are much harder to trace and then far harder to connect you with them. 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, 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.

C. 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 increased 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 neighbouring town to do the printing and photocopying.