14.5 PURCHASING MOBILES ANONYMOUSLY

To ensure anonymity take the following precautions when buying a mobile phone:

- Make your purchase in a shop away from where you live.
- Try if possible to avoid town centres where there is a greater likelihood that you will be on CCTV. Many small or second-hand shops do not have cameras and those that do are unlikely to retain tapes for longer than a week if at all. High street shops & supermarkets will keep CCTV footage for much longer. Follow the general guidelines for purchasing equipment (see previous section).
- Do not give real details if asked. Many shops do ask for personal information, but do not require proof of ID. In countries such as the UK this is not actually required as yet, and is done under the guise of marketing or for anti-theft purposes, but you are entitled to refuse. However, in order to draw less attention it is probably better to give false information.
- Go for simple phones without all the extra features now being made available.
- Pay with cash.
- Do not register the phone if you do not have to, or else give fake/alternative details, preferably the same ones you have given the retailer.
- Burn all packaging. Most packaging carries various bar codes that permit a particular phone to be associated with it and thus where it has been sold, etc.

Topping up credit

When setting up the mobile, use pay-as-you-go options where possible; this is a more expensive solution, but is much better for anonymity. As with any purchase, this can be used to link you to the purchase and thus to the phone, so follow the same guidelines for other equipment - avoid CCTV, wear nondescript clothes, baseball caps, etc and pick smaller shops. Use cash to purchase top-up vouchers rather than credit cards / ATM machines to top-up swipe cards. Burn or otherwise securely dispose of any top-up vouchers, etc.

15. CONCLUSION

Remember, security is about empowering yourself to take action in today’s repressive society. If you are not taking action, then your opponents have won. There is no such thing as a foolproof system, and there will be an element of risk to everything you do, but do not be put off by this.

At the end of the day we are all motivated by a desire to change the world for the better and that is something that takes courage to do in the first place. You have already made the important steps, so please take away from this and the knowledge to keep making those steps towards your goal. Be empowered, keep fighting and stay free.

If you don’t understand some points or need further help, always ask. It is better to be safe than sorry.

The authors have kept themselves active and free for many years now, so there is no reason why you cannot do the same, without making their mistakes.
A Practical Security Handbook for Activists and Campaigns

version 2.5

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

14.3 Network analysis

There is a third class of risk associated with mobile phones and that is analysis of patterns associated with their use. This can be done to a limited extent with land lines, such as whom do you phone the most and when, but with mobile phones there is a greater scope due to the changing geographical factors. In particular, this allows phone to be associated with a household or individual, even if that phone has been registered as pay-as-you-go. Other information such analysis will provide includes the particular network of contacts associated with that phone and thus it’s owner.

Once a phone is used it hooks into the network. So if you use your new mobile to call the land line or mobile of a known activist, your phone is marked for attention. The more it is used in such a fashion the more that phone is compromised and linked into the network. Thus once the phone is used in this fashion then it should be considered compromised, even if you’ve taken care not to have your name associated with it.

Where and when phones are turned off is also telling. If everyone goes to a meeting place then turns off their phone that is a clear signal that something is up in that area. Likewise, if one person is being tracked to a meeting place, those monitoring them can see if other phones in that cell are switched off at the same time, thus giving them insight into the potential network of individuals associated with their target. Similarly at a meeting, knowing the phones there can be use identify the individuals present. It does not even have to be a meeting – it can be the fact that you’ve visited someone’s house so making a connection between the two of you.

From another angle, if a selection of known phones appears in the same cell or nearby cells and then get turned off it is an indication that something is taking place.

The best solution if you don’t want to be associated with a meeting is to leave your phones at home (switched on), or turn them off some time before you get to the designated area.

14.4 Mobile phones and activism

The above sounds somewhat frightening, and it is meant to be. In our view, mobile phones pose a considerable risk and facilitate state monitoring of us. They are in the process of trying to phase out pay-as-you-go phones on a regular basis. Purchase pay-as-you-go phones in a secure manner (see below), and avoid registering them in your name. Governments are in the process of trying to phase out pay-as-you-go phones so all mobile phones will be registered to individuals. If your country requires a phone to be registered, consider using addresses of friends/squats and false names; swap phones with friends on a regular basis as well.

If you are arrested with a phone you can be sure of two things – the police will forever associate that number with you and they will go through the information on it, including text messages, recent made/received calls, and address book. Calls made during the time of the action will clearly place other phones in the picture and if the police can put names to those holding those other phones then it puts them in the firing line as well. Thus if an action is going wrong, get rid of your phones as soon as possible, preferably securely. What you should not do is ring a land line to say that you are in trouble. Better to wipe free of fingerprints and dump it first.

14.4.1 Meetings

Depending on your required security we recommend the following list of action to be taken, graded in terms of increasing risk

a) Turn off all phones.
b) Place in a box in another room.
c) Remove batteries.
d) Turn off before well before getting to the meeting place.
e) Leave at home altogether.
f) Give to someone else to take elsewhere.

14.4.2 Covert Action

For all our negative opinion on phones, we do accept that they play a valuable role in activism in terms of keeping disparate groups in contact or for use on actions.

The trick is to create a network of phones that are not linked into any other networks. This is known as “closed network” and has been used very effectively by different groups of activists. If the risk associated with being caught is great then it is worth investing in a set of phones to create a closed network solely for that action and following the guidelines set out below.

• Follow the guidelines for purchasing mobiles securely
• Ensure that none of the phones in the network are used to ring any of your friends or contacts, or indeed any phone outside of the network. Once this happens the network should be considered compromised and the phones disposed of (sold on/trashed).
• Keep the battery out when the phone is not required for use.
• Keep the SIM card out when the phone is stored, preferably in a separate place from the rest of the phone; important in case there is a raid.
• Never turn the phone on in your house, office or regular meeting places as it will immediately be associated with that place, especially if it is the first location turned on in. If you suspect your car is under surveillance then avoid using the phone in or near it.
• Avoid patterns of phone use – for example always using the same area and/or time to make the phone calls.
• When making phone calls avoid areas where there is CCTV; consider a bike ride into the countryside, etc, or finding an enclosed bus shelter.
• Avoid spending longer than 30 minutes in one area when using the phone. Make use of the fact that the phone allows you to be mobile.

To help defeat the various risks associated with network analysis change your phone number and phone on a regular basis. Purchase pay-as-you-go phones in a secure manner (see below), and avoid registering them in your name. Governments are in the process of trying to phase out pay-as-you-go phones so all mobile phones will be registered to individuals. If your country requires a phone to be registered, consider using addresses of friends/squats and false names; swap phones with friends on a regular basis as well.

14.4.3 If arrested:

If you have your mobile phone with you, take the following steps:

• Keep the phone off.
• Remove the SIM card.
• Keep the phone safe. Use a tamper proof container if possible.
• Keep a list of all numbers, addresses, and passwords (see below).

To help protect the various risks associated with network analysis change your phone number and phone on a regular basis. Purchase pay-as-you-go phones in a secure manner (see below), and avoid registering them in your name. Governments are in the process of trying to phase out pay-as-you-go phones so all mobile phones will be registered to individuals. If your country requires a phone to be registered, consider using addresses of friends/squats and false names; swap phones with friends on a regular basis as well.

14.4.4 Analysis:

If you are arrested with a phone you can be sure of two things – the police will forever associate that number with you and they will go through the information on it, including text messages, recent made/received calls, and address book. Calls made during the time of the action will clearly place other phones in the picture and if the police can put names to those holding those other phones then it puts them in the firing line as well. Thus if an action is going wrong, get rid of your phones as soon as possible, preferably securely. What you should not do is ring a land line to say that you are in trouble. Better to wipe free of fingerprints and dump it first.

14.4.4 Covert Action

For all our negative opinion on phones, we do accept that they play a valuable role in activism in terms of keeping disparate groups in contact or for use on actions.

The trick is to create a network of phones that are not linked into any other networks. This is known as “closed network” and has been used very effectively by different groups of activists. If the risk associated with being caught is great then it is worth investing in a set of phones to create a closed network solely for that action and following the guidelines set out below.

• Follow the guidelines for purchasing mobiles securely
• Ensure that none of the phones in the network are used to ring any of your friends or contacts, or indeed any phone outside of the network. Once this happens the network should be considered compromised and the phones disposed of (sold on/trashed).
• Keep the battery out when the phone is not required for use.
• Keep the SIM card out when the phone is stored, preferably in a separate place from the rest of the phone; important in case there is a raid.
• Never turn the phone on in your house, office or regular meeting places as it will immediately be associated with that place, especially if it is the first location turned on in. If you suspect your car is under surveillance then avoid using the phone in or near it.
• Avoid patterns of phone use – for example always using the same area and/or time to make the phone calls.
• When making phone calls avoid areas where there is CCTV; consider a bike ride into the countryside, etc, or finding an enclosed bus shelter.
• Avoid spending longer than 30 minutes in one area when using the phone. Make use of the fact that the phone allows you to be mobile.
Some are, however, understood somewhat better. One such feature of various Nokia phones is that they are easily adapted to be turned on remotely without alerting anyone. These models are still being sold in various shops specializing in surveillance equipment, and have the advantage of being very common. They are generally sold along the lines of people leaving meet- ings to go to the toilet, leaving their phone behind in the room. They ring the phone remotely, it turns on and the phone owner can hear what is being said in the room. It is not a great leap from there to getting someone else’s phone and turning it on remotely to hear what is being said nearby.

As phone software develops it becomes increasingly open to being hacked in much the same way as computers. Software technologies exist which place ‘active monitors’ in a room and identify  theirs various makes/models. With this information, carefully tailored signals can be sent to particular phones, prompting the owner to apply security patches, updates, etc. This also allows harmful malware ("malware") instead, thus putting the phone under the control of a third party. A simple bit of malware is one that monitors the phone’s address book, providing the interloper with its details and then notify when it has been updated. For ordinary mobile phones with basic functions, this is not a significant problem; for more sophisti- cate phones that permit access to emails and internet it is a much greater risk.

Different phones offer other features which can be used against the campaigner - a good example is GPS systems which allow accurate positioning of phones and thus their users/owners.

The software poses other simple hacks for unsuspecting users, which again depend on networks and models. In a recent case a UK reporter was able to access the messaging services of a phone to receive a message or call it needs to let a mast know which again depend on networks and models. In a recent case a UK reporter was able to access the messaging services of a phone to receive a message or call it needs to let a mast know which again depend on networks and models. In a recent case a UK reporter was able to access the messaging services of a phone to receive a message or call it needs to let a mast know that it is in its cell. It will send out a broadcast signal and select the strongest reply as the nearest mast to communicate with. This location is logged so when there is a message or phone call for that number, the network can route directly to you. A mobile phone on your car’s dashboard may cause your radio speakers to emit a hissing sound as it sends its location to nearby masts as it changes from one cell to another.

Locating a phone in a particular cell gives the network a rough geographical location of the phone’s position. If there are several masts in an area and they all pick up a signal from a mobile phone, then triangulation techniques can be used to pinpoint the location of the mobile phone more accurately. The higher the density of masts the easier it becomes, so in a city this technique is far more accurate than in the countryside.

A good place to make locating the phone more difficult is on a motorway were the cells tend to be in long lines which makes triangulation difficult. Another place which confuses the system is to be directly underneath a phone mast which also confuses the process by removing helpful data from other masts. This feature of communication is going on all the time and is what turns a mobile phone into a tracking device. In the UK all these exchanges are being logged by the various networks at the request of the government and by law. In the US, “en- hanced 911” features are required by law to allow emergency services to track the location of a mobile phone, though of course this is open to abuse by others.

This feature is being turned into a commercial application. There are firms which actively track mobile phones of em- ployees on behalf of their bosses to ensure the employees are where they say they are. It is also marketed to parents as location devices for their children. In theory this is done with the consent of the phone holder/owner as they have to send back a text acknowledging the service. However, this is simple enough to circumvent if they are not in possession of the phone.

The higher the density of masts the easier it becomes, so in a city pinpoint the location of the mobile phone more accurately. In the countryside, the network can route the call, the phone number called, and the contents of any text messages. If there are any other features enabled, such as address book back-ups, then they are also recorded.

UK legislation, in particular the 2001 Anti-Terrorism, Crime and Security Act, demands that networks keep logs of various bits of this information. Time, duration and numbers called are kept away for billing purposes (BT keeps all such in- formation for 6 years); texts are kept for 6 months (and in the UK are admissible in court whereas actual phone calls are not) and URLs for 4 days. The particulars of other information to be stored are currently under negotiation with the various companies involved. Of course all such stored information is open to the police and other security services to access. The EU is also looking at bringing in similar legislation, though there are data retention issues. In the USA, there is no data retention issue and corporations can keep information for as long as they like, and often do.

As with landlines, the technology to listen in to mobile phones is readily available to the state, and a number of companies are increasingly tapping activists in countries as well other than their own. In the UK mobile phone networks have implemented various protocols in their systems that actively facilitate government agencies to listen in on phone calls. The basic advice is to treat mobile phones with all the circumspection you would land- lines. You wouldn’t say anything incriminating over your home or office phone, so don’t start doing it with mobiles either.

There is another threat with mobile phones, albeit rarer. It is possible to step in between a phone and a mast by using an appropriately set up computer as a relaying station, which emulates being a mast. If it is close enough to the target mobile phone, the phone will route its communications with the network through it without realizing anything is amiss. The person in control of the router then has access to everything that has been sent, including the conversation and numbers. This feature is being turned into a commercial application.

Security For Campaigns

Basic campaign security

Media strategy

Your address

Answering emails, letters & phone calls

Websites

Keep files encrypted

Need to know

Office security

Advanced campaign security

Burning rubbish

Paper trails

Sources

Backups

Tampering

Anonymous structuring

Communications

Meetings (Basics)

Meetings (High Security)

Secure information transfer

Gossiping

Being monitored

Dealing with infiltrators & grases

New People

Do you have an infiltrator

Initial action & gathering evidence

Exposing the infiltrator

Dealing with the fallout

Gatherings

Grasses after arrest

Other infiltration methods

Security for demonstrations

General Rules

Evidence Gatherers & FIT

Cameras

Travelling to demonstrations

Debriefing

First Aid

Dealing with Provocateurs

Personal security

Dealing with the police

At Home

Control the information in your house

Preparing for a raid

Phones, computers & emails

Buying

Being aware of intruders

Being bugged

Your area and neighbours

Your car

Self defence

Surveillance

Preparation for surveillance detection

Vehicles

On foot

Rural surveillance

Counter-surveillance

Baltant surveillance

Computer security & Internet privacy

Security

Internet Privacy

UK legal issues

Regulation of Internet Powers Act

Talking to others about security

Future shocks

Closed culture vs. open culture

Writing letters

Mobile phones

15 Conclusion

Final note, contact details & disclaimer

TABLE OF CONTENTS

1. Introduction

1.1 Why security is important

1.2 What is security?

1.3 Setting up the ‘security process’

2. Security for campaigns

2.1 Basic campaign security

2.2 Advanced campaign security

3. Dealing with infiltrators & grases

3.1 New People

3.2 Do you have an infiltrator

3.3 Initial action & gathering evidence

3.4 Exposing the infiltrator

3.5 Dealing with the fallout

3.6 Gatherings

3.7 Grasses after arrest

3.8 Other infiltration methods

4. Security for actions

4.1 Choosing people

4.2 Getting out of the area

4.3 Planning

4.4 Acquiring equipment

4.5 Clothing & other traceables

4.6 Disposing of equipment/clothes

4.7 Communicates & photos

4.8 Mobile phones

4.9 Police boxes

4.10 Travelling

4.11 Being Chased

4.12 Using entry-gaining tools

4.13 Debriefing

4.14 Shitting in your backyard

4.15 Debriefing

4.16 Making a phone call

4.17 Conclusion

5. Security for demonstrations

5.1 General rules

5.2 Evidence Gatherers & FIT

5.3 Cameras

5.4 Travelling to demonstrations

5.5 Debriefing

5.6 First Aid

5.7 Dealing with Provocateurs

6. Personal security

6.1 Dealing with the police

6.2 At Home

6.3 Keeping the information in your house

6.4.1 Preparing for a raid

6.4.2 Phones, computers & emails

6.4.3 Mail

6.4.4 Being aware of intruders

6.4.5 Being bugged

6.5 Your area and neighbours

6.6 Your car

6.7 Self defence

7. Surveillance

7.1 Preparation for surveillance detection

7.2 Vehicles

7.3 On foot

7.4 Rural surveillance

7.5 Counter-surveillance

7.6 Balian surveillance

8. Computer security & Internet privacy

8.1 Security

8.2 Internet Privacy

9. UK legal issues

9.1 Regulation of Internet Powers Act

10. Talking to others about security

11. Future shocks

12. Closed culture vs. open culture

13. Writing letters

14. Mobile phones

15 Conclusion

16. Final note, contact details & disclaimer

43 of 45
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 with a backlash. Government enforcement agencies and corporations all have vested interests in criminalizing, disrupting and suppressing activist groups of all persuasions. Security is needed to ensure our continued success. We also have a basic right to protect your privacy and anonymity from unwanted intrusion.

For those who say that we shouldn’t have anything to hide or shouldn’t make a big deal out of it, it is our hope that the world democracy is subverted daily and the people doing it are more likely to be those in power. As long as governments and their supporting apparatus permit corruption through their closed and secretive nature then we need to respond in kind for our own protection.

Threats do not just come from the state. There are situations were media organisations with their own agenda will attempt to target campaign groups. Private investigators also need to be factored in as threats. Both have distinct issues which also need to be factored in. And you need to be prepared for this. Once you have decided on the appropriate security process, there is no room for shortcuts. Going out of your way to avoid compromising you, yes, there are times when you are just too tired to encrypt all your sensitive files, but that is one half hour compared to the prison sentence which may await you should you get rained the following morning?

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

1. **Security is a Process that Protects You in Some Fashion, Whether in the run up to, during or after the event you are involved in.**

This means, that security is there to facilitate the smooth operation of your action, campaign, etc. and help keep everyone safe.

A common mistake is equating paranoia with security. Paranoia is often used as an excuse not to take action through fear. This is no longer enough to combat the omnipotence of opponents. In our experience paranoid people have little to fear as they are too nervous to do anything that works. You really put them at risk if you do not take basic security measures put in place. This sort of fear means you effectively defeat yourself.

There is no such thing as a 100% fail-safe system, and no doubt there is a reason that you cannot call it fail-safe. A system is not an excuse for coping 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 problem and a state of mind. You cannot put down and pick up security at whim. For security to be effective and worth the time and effort put into it, it has to be built into your life. Ideally, it becomes second nature; that is what we try to help you achieve. You need to become your own security. This creates a mindset that helps you avoid errors of judgement you may regret later. There are objects and software that will aid your security buying them is not enough - you need to secure it in itself; they need to be part of an active security process. For example, there is no point having a bug scanner if you don’t set it on a regular basis. Likewise anti-virus software will not protect your computer unless it is 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 an action is too late. Hence, when you start planning, think about the situation and the threats that may arise, so you are incorporating features that protect your security as you go along. It makes protecting yourself easier and means you are less likely to make mistakes.

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

\[
\text{Security} = \text{Time} + \text{Effort}
\]

You cannot get around this basic fact; every security measure will have some sort of impact on your life, including work. Security measures may require you to put in more time, and effort. This will be more and more time, and effort as you go along. It makes protecting yourself easier and means you are less likely to make mistakes.

1. **What is Security?**

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

Security is a process that protects you in some fashion, whether in the run up to, during or after the event you are involved in. Activities have conflicting opinions on the risks associated with mobile phones, ranging from considering the security risk from them to be negligible, to keeping them at arms length as much as possible. Backing up your mobile phone is not considered by many experts a priority. One expert who works with a wide range of corporations, including the police. His advice was that for all our worries and fears we have a lot to be thankful for - it’s worse than we thought. When it comes to activism and mobile phones, leave yours at home. We consider that good advice. Like everything there are exceptions, but with mobile phones good practice is to treat them with the utmost suspicion from the start.

11.4.1 *Inside a mobile phone.*

A mobile phone is a complicated beast, and is getting even more so as technologies converge. From a hardware perspective, there is

- the battery
- the SIM card
- the phone itself

The battery is the main power supply for the phone. People often recommend removing it so the phone will not work. This is not necessarily the case. Secondary batteries to keep your mobile phone going are available. If you use these batteries to keep your phone going, they will help you to bypass the phone’s security system.

Alternatively, if the battery is bad, you could use a secondary battery to keep your phone going. If you do save the file, never simply delete it as this does not act to remove it from your computer. Instead use a dedicated wipe programme such as PGP Wipe or Clean Disk Security to remove it fully from the hard drive. Better still, if saving it, do so to a floppy disk that can be burnt if necessary. Make sure that the number of wipes is set to at least 8 or 9.

Finally, if writing something of a particularly sensitive nature then use the free space wipe options in the above software to be on the safe side. It is good practice to run free space wipes regularly to make sure that there is nothing awkward left behind on your computer disk. Though be aware it will shorten the life of your computer’s hard drive.

Alternatively, if the environment is safe enough, then use a uni-

versity or library computer, so there is no connection to your own computer.

1.3.2.2 *Printing.*

Printer and especially typewriters have their own fingerprints. This makes it very easy for there to be a letter and an address held in the 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 easier to find out who connected with you. You can type the letter up at home, and bring it in on a printer.

Some problems with this are people looking over your shoulder to 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 do not want to touch the actual letter or have others see it. To avoid the obvious wear-

ing 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 the obvious look of a printout.

Finally, if you type the letter, put in a page or two of gar-

bage text at the beginning and end of your letter to achieve the same effect.

1.3.2.3 *Photocopiers.*

Finally, once you have your letter printed off, a very good tech-

nique to adopt is to photocopy it. This will help avoid telltale

printer marks by obscuring them with the photocopier’s own fin-

erprints. To enhance this, put the page on the printer at a slight

angle, alter the contrast a little and maybe put the photocopier

down half way through an action in a blurry effect even fur-

ther. 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.
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 a nightmare to security agencies as it is a dream for the activists. Unfortunately for us, their resources are rarely up for more than cursory work unless a political decision is made to focus on a particular group, a lot 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 you are talking to or have travelled with.

Mistakes happen, even to experienced activists. It is a fact of life, especially when doing actions under stressful situations. This is not to say that you should not do these things, but it is important to acknowledge that a mistake is not an excuse to down tools. If your security process is set up right, it should be able to tolerate mistakes and work through them. There are a number of mistakes that can completely jeopardise an action, but not every mistake is in this category, and you should recognise the difference.

If someone makes a mistake, let them know but don’t treat them as a pariah on the basis of one; the time to get concerned is when mistakes are being made repetitively and they are missing an effort to learn from them, even when pointed out.

Finally, sit down and take time to plan your security needs and how they will impact on your life and your activity. Besides a willingness to take the time and effort to achieve good security, good planning is the other key feature. 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 lose 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 aims to change the status quo in some fashion means you are a threat to those who currently enjoy the status quo. We have already seen quite a number of things you can do, all legal, which will help maintain your privacy. Below is an account of how one person worked to put together some guidelines. Not everything they do is necessary – play it by your own needs and situation.

13. WRITING LETTERS

Even writing letters can get you in trouble these days if you are not careful, especially when companies and the like can afford to plough through your own data and build up a profile. There are quite a number of things you can do, all legal, which will help maintain your privacy. Below is an account of how one person worked to put together some guidelines. Not everything they do is necessary – play it by your own needs and situation.

13.1 WRITING LETTERS AT HOME

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

I tend to purchase my material out of town from well-known sources (not fussing about 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 any ‘nose’ effects (eg perfume, cigarettes, etc). The table is washed down and disinfected (cheap vodka or white spirits will do); the floors hosed 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 your 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 hands clean.

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 normal handwriting. Watch out for examples in your letters that act as tell-tale signs of who you are.

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.

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, add an extra one for each letter (so if you sneeze or do something like that, then these will not have to be scraped). As with envelopes, use self-adhesive stamps; not the sticky type as these are a potential giveaway.

Post out of town, try using a different postbox each time, preferably ones not in town centres where there are CCTV cameras. Countryside ones are good. To avoid getting fingerprints on the envelopes as you post them, use the plastic bag to dump them in the post box (doesn’t look as obvious as gloves in warm weather).

13.2 COMPUTERS, PRINTERS & PHOTOCOPIERS

13.2.1 Computers

On the computer, use simple text editors such as NotePad on Windows, SimpleText on Macs or emacs/vi on Linux. Big programmes such as Microsoft Word, Lotus Notes, etc often store backups of your text, and have a variety of issues that you may not even be aware of. If you haven’t done so already, get a password on your computer so that 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 Microsoft Word or similar software.

Where possible, do not save the file; some systems will allow you to print off a file without saving it first. With the simple

13.3 SETTING UP THE ‘SECURITY PROCESS’

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

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 may not feel comfortable about doing that, but at least you have not left a clue as to who the letter is from. Don’t put your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your leaving less of a trail. Using the plastic bag to wrap the letters carefully taking your time over them if necessary. The letters are not opposed to this, and on some levels it is an advantage to have people at actions as well and on the organisational front are a nightmare to scupper by your opponents. Larger meetings make it harder for infiltrators to be picked up and also makes it harder for them to know who you are. 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 may not feel comfortable about doing that, but at least you have not left a clue as to who the letter is from. Don’t put your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your leaving less of a trail. Using the plastic bag to wrap the letters carefully taking your time over them if necessary. The letters are not opposed to this, and on some levels it is an advantage to have people at actions as well and on the organisational front are a nightmare to scupper by your opponents.

Larger meetings make it harder for infiltrators to be picked up and also makes it harder for them to know who you are. 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 may not feel comfortable about doing that, but at least you have not left a clue as to who the letter is from. Don’t put your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your leaving less of a trail. Using the plastic bag to wrap the letters carefully taking your time over them if necessary. The letters are not opposed to this, and on some levels it is an advantage to have people at actions as well and on the organisational front are a nightmare to scupper by your opponents.

Larger meetings make it harder for infiltrators to be picked up and also makes it harder for them to know who you are. 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 may not feel comfortable about doing that, but at least you have not left a clue as to who the letter is from. Don’t put your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your leaving less of a trail. Using the plastic bag to wrap the letters carefully taking your time over them if necessary. The letters are not opposed to this, and on some levels it is an advantage to have people at actions as well and on the organisational front are a nightmare to scupper by your opponents.

Larger meetings make it harder for infiltrators to be picked up and also makes it harder for them to know who you are. 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 may not feel comfortable about doing that, but at least you have not left a clue as to who the letter is from. Don’t put your fingerprint on the letter so not writing the letter in the first place, but you are setting up a process which facilitates your leaving less of a trail. Using the plastic bag to wrap the letters carefully taking your time over them if necessary. The letters are not opposed to this, and on some levels it is an advantage to have people at actions as well and on the organisational front are a nightmare to scupper by your opponents.
to focus just on the threat from a politically motivated police, but these are not just the only risks (think media exposés, etc.). However, most of the techniques dealing with the various threats are complementary.

That the principle threat is often the state has lead people to 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 security 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 makes it much easier for the campaign to be infiltrated and disrupted. Resources will then be directed at your most vulnerable points and key personnel. Disruption can either be anticipating your campaigns tactics so effectively countering them and undoing all your hard work, or else causing splits within the group. It can also involve the arrest of 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 think about how your campaign can be better secured.

a. Don’t boast about your own security precautions. Security is about trusting others to look after it, and that weaknesses are minimised according to the threat you are likely to face. However, there are no guarantees so be prepared to walk out if you go too far.

b. If you go over the top, then you risk putting people off, scaring them or otherwise disempowering them. Encourage people in your group, especially those less experienced than yourself, to think about their security needs, and how lapses in security can affect other people but don’t enforce without explanation. Be wary of letting a ‘more-secure-than-thou’ competitive attitude develop as in a group as that is very off-putting; likewise with installing a paranoid mindset rather than an active one.

c. As a campaign, you need to discuss security in a dedicated meeting and reach a consensus on it. Dictating security only

i. In one case, an activist was approached by a media organisation about providing some insight and help protect you from fellow campaigners feeling at odds with them.

j. There is also important to ensure new or temporary volunteers are also brought up too speed, before they start working for you, you may not have a team with everyone being patronising about security. It is also important to ensure to protect your

ii. As technology develops, there will be advancements in methods of transport and not just a meaningless chime 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 to handling the media. They will have a better sense if the call is genuine and will be better able to deal with the tricks of an interrogator. You 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 change it. It is a good idea to change both first and second names otherwise you just end up being known by the pseudonym, which defeats its purpose.

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

Press releases can be treated the same way. Consider disinformation by using false names and place persons. Disruption can either be anticipating your campaigns tactics so effectively countering them and undoing all your hard work, or else causing splits within the group. It can also involve the arrest of activists, theft/damage of equipment and smear campaigns.

10. TALKING TO OTHERS ABOUT SECURITY

It is important to discuss security in your group. You need to make sure that everyone in the group understands that there is a need for security measures even if they do not

a. If you see a security lapse in someone else, there are several ways of dealing with it:

i. Bring it up as a general point at a meeting in a setting where it is not some one picking a fight or shaming. This has the advantage of reminding oth

ii. Take the person aside and explain your concerns, explaining that you feel uncomfortable and why. In particular, say that it is not they who are at fault.

j. 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.

k. Don’t take security all as seriously as you do, nor rely too much on your security. 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.

l. Don’t give bad advice, or make things up rather than appear ignorant. Security can change quite rapidly, especially with scary developments like RFID chips, improved biometric techniques, etc. If you don’t know the answer then it is better to say so, than to lead someone into a false sense of security.

m. 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 internal information, then they are probably better to lapse. Give them a chance to change, but if they don’t, then make 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 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 used to disseminate information, for 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 transport and not just a meaningless chime they are being forced to go through. Cooperation is the keyword here.

a. Improved forensics catching traces that would have been missed on materials, etc previously.

b. Improved data exchange between police organisations and between police and various other keepers of personal information such as banks. This also includes improved processing and cross-referencing of information (see also point 8.)

c. Increasing sophistication of listening and tracking devices, in particular in transmission range and in miniaturization of them (e.g RFID tags). Though the technology has been around for some considerable time, it was not always
8.2 Internet privacy

Internet privacy is never left unattended at any time. If you suspect that you are going to attract this sort of attention, use a prepared infiltrator so encryption of anything sensitive is a must.

- Do not base them on the names of family, pets or dates of birth.
- Include a mixture of dictionary words or sequences of letters/numbers which are essentially random.
- Really sensitive material should be protected with passphrases of a minimum of 16 characters from the entire range available – including upper and lower cases, numbers and any permitted symbols.
- Change them on a regular basis.
- Do not write them down and stick them under your chair or desk – these are the first places that an intruder will look.
- Back up your computer in case it is stolen but keep the back-ups secure somewhere else.
- Consider switching away from Windows to other operation systems such as Linux or Mac which have better security features.
- Avoid wireless keyboards as they transmit quite a distance and are being monitored, do not do anything sensitive from your home computer. Watch out for CCTV in internet cafes.
- Consider switching away from Windows to other operation systems such as Thunderbird (recommended), Eudora or Pegasus. Outlook is notoriously buggy and a significant agent of virus transmission.
- Avoid using Internet Explorer to surf the internet – use an alternative such as Firefox. It is tempting to avoid using Internet Explorer, switch off Java and ActiveX.
- 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 cafe. If you suspect you are being monitored, do not do anything sensitive from your home computer. Watch out for CCTV in internet cafes and media such as memory sticks.
- 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, 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 question your own conclusions on your behaviour, but there is no law to stop you taking preventative measures.

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

Know your law – it will keep you from getting arrested and by knowing your rights you can protect yourself much better when you are approached by the police, or being searched (particularly late at home). For up-to-date information on the state of play with law in England and Wales visit www. freebagels.org or www. activistsinfoelproyect.org.uk. If you are based in Scotland then the law is different – check out http:// g8legalsupport.info/2005/03/08/an-activists-guide-to-scots- law and www.tridentploughshares.org.uk

Keep an eye on forensic issues & standards of evidence in court. This can be picked up from news stories of high profile convictions and also websites. Knowing this will inform how you decide when balancing up risks.

9.1 Regulation of Internet Powers (RIP) Act

The main issue for campaigners here is that if they seize your computers, then they have the powers to demand that you surrender the passwords to your computer and any encryption techniques you are using. Failure to do so in theory can result in a two-year prison sentence.
names and descriptions of roles. However, also consider how you put them 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 encryption or disk encryption.

F. Need to know.

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

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

G. Information Management

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

• Have policies 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 particular is letters from other people, etc).

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

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

H. Office Security

When you move into a new space, secure it. Change all the locks, possible break-ins can and still occur with a variety of lock pick sets. Likewise your nameplate should be aware of what sort of information casual visitor may also be able to obtain from near your office:

• 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 sensible underhand, do not do it from near your house/office either as these are just as likely to be bugged.

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

• 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 procedures 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 means that you are unable 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 know well where your office is and have access to it. If you must let relative strangers in don’t leave them alone. 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 sources 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 these so people cannot squeeze through. The state and professionals will have little problems with most locks so it is important to ensure that security does not simply stop at the door.

2.2 Advanced Campaign Security

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

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

When burning paper, do so until it is white and then scatter it lying around (in particularly if is letters from other people, etc).

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

b) Paper trails: watch out for leaving paper trails when you destroy literature & memoranda. If your literature becomes a point of contention or you would rather it remained anonymous in relation to your campaign, work out a plan that either stop them locating your printer who can in turn point to you, or else keep your printers at arms length. That is, do not use your phones, personal mobiles or campaign addresses were possible. Collect in

if they are innocent and will pretty much react in the same startled way, thinking you are a mugger. However, you can get up close and ask for directions, a cigarette light, etc which will in general further away and there is much greater scope to hide, especially if there are thick woods nearby. A surveillance team will:

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

Things to check for are:

• Repeated glints off binoculars from woods or copse.
• Abandoned buildings where they are using to hide vehicles.
• Transmissions from cameras.
• Flattened grass and depressions; also vehicle tracks where they shouldn’t be.
• Identify potential observation points from your location and regularly check them – it may discourage the surveillance team from using them or getting too close.

• Walk in an ever widening circle, looking for places of concealment focusing on places such as tree-lines, copes, thick bushes/hedges which have a view of the target area.

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

7.4 Counter-surveillance

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

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

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

• The surveillance team may be aware of who your friends are so will be able to recognise their faces; if engaging in this it is sometimes more effective to adopt a sort of change of your normal appearance or disguise.

• The security around the set up needs to be very tight – if you are meeting up to plan it, the meeting needs to be tight so that the surveillance team doesn’t get wind of the idea so keep a core group.

• The counter-surveillance team needs to be able to move swiftly and discreetly; this includes hand signals that are not likely to be seen by people (eg, outstretched hands as opposed to a quick scratch of the chin).

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

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

7.5 Blatant Surveillance

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

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

8. Computer Security & Internet Privacy

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. However, as a bare minimum you should be doing the following:

8.1. Security

• Install and regularly update anti-virus and firewall software.
• Install a password manager such as 1Password (www.1password.com) and ZoneAlarm (www.zonealarm.com) are available for Windows. The important feature is that live update is activated, it will in general automatically get updated.
• Install spyware detector programmes such as Ad-Aware which is free from www.lavasoft.de.
next to exit and watch for people following you being startled by you waiting for them (in turn) and anti-surveillance as it gets you out of sight long enough to get away. This works best with shops you don’t go into, or if you do, you always use the same entrance and exit.

e) Elevators that take you to other floors with exits are good; remember that the surveillance team will leave someone at the ground floor in case you return there.

f) Places where there are security checks can work in your favour, especially where there are multiple exits/entries. This surveillance team will be reluctant to set off alarms with their communications gear. The delays for stop and search also play into your hands.

At night be prepared for the increased use of technology such as infrared to monitor you.

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

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

Public transport

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

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

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

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

Beware of chance encounters with strangers, especially those who appear to have something in common with you, where strong flows of people in one direction. If you move against this flow, watch out for others doing likewise and struggling to keep you in sight. As you have to look as you do this, it is an active detection technique.

Night surveillance while on foot

This is a much different situation from day time foot surveil- lance. A professional, depending on your advantage, depend on crowd density and how well you can push through them.

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

Driving without lights

• Light going on and off in stationary cars
• The sound of radio transmissions
• Doors slamming shut as you approach
• Vehicles parked in unusual places
• Couples sitting in cars, staring straight ahead rather than engaging with each other.
• Sitting for prolonged times with the engine running.

Surveillance teams have been known to use taxis and police cars in the same situation. If you know your area well then you can spot them by being parked in places not normally used by them. For instance, police cars do not normally hang out in well-to-do estates. Taxis do not wait on poor and out of the way estates. People waiting on friends at nearby houses tend to your advantage, depending on crowd density and how well you can push through them.

Some tactics that work better at night are as follows:

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

• You have more opportunities to conceal yourself and watch the reactions of suspect tails as they realize that you are not in sight. Remember, that if you confront someone then person and pay in cash (which may get you discounts as well). Destroy receipts as well where possible.

• Sources are a vital resource to most campaigns, and a very easy point to discredit you if it can be shown that you provided them with false information. 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 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 meet- ings in your office or for unusual hours. If you are using an anonymous place away from your office and homes. Burn notes as soon as they are typed up (and encrypted), and store them in an anonymous place away from your office and homes. When referring to sources use a codename and keep their real identities as secret as much as possible. Work on a need to know basis and discuss their existence as little as possible. Don’t pub- lish their work without their consent first.

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

• Back-ups of your information and material are vital to keep your campaign alive. If you were to lose your mem- bership list, keys or talk about inside sources, then why tell them, or at least without making them feeling excluded. If they don’t need membership list or research for whatever reason, accidental or maliciously, then it is potentially a crippling set back. Keep this sort of information backed up and your back ups something that they have to steal. It is also something that you can push through them.

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

Night surveillance while on foot

This is a much different situation from day time foot surveil- lance. A professional, depending on your advantage, depend on crowd density and how well you can push through them.

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.

Finding out who is attending meetings is just as impor- tant as what is being said to those monitoring you, as it allows them to build up a list of people involved in the group. So if you do not want to be visibly associated with a group this is something to bear in mind.

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

a) Don’t use a pub, especially ones commonly frequented by other activists or which are likely to have the police monitoring it, especially if they are going to bug your phone at the office or home, the chances are they will also tap the phone boxes. Do not give away too much information to your remote phones may be any- noying, but it will also make life a lot more difficult for those monitoring you, but avoid favouring one.

b) Your communications may be tapped, and not just by the state. Don’t say anything on the phone, or in emails, letters which could compromise you or anyone else. It is certainly worth considering campaign tactics and names people as carrying out specific responsibilities, certainly not real names anyway.

Be prepared to purchase mobiles that are only for specific tasks such as sources and do not use them for other campa- ign 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. Do not give away too much information to your remote phones may be any- noying, but it will also make life a lot more difficult for those monitoring you, but avoid favouring one.
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 little bits and pieces 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 out for topics and not ones completely different). Avoid fidgeting and rushing off.

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

d) If you arrive at different times, do no hang around waiting to be picked up outside your meeting in – it makes it obvious if 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.

The most secure way is to arrange a meeting is by word of mouth (never over the phone/text/email) to assemble at a meeting point twice or otherwise creating pattern.

If your group has regular meetings, arranging to meet immediately afterwards to discuss something more serious might not have complete control over visibility.

Don’t over complicate things as that leads to mistakes. Be obvious about it (look for related topics and not ones common). Avoid hanging around and attracting attention. Finding the place and going somewhere else is 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, including many drops where information can be exchanged without parties meeting each other, etc. However, these are more useful for situations where knowledge of contact is the most important things to be avoided, or all that is being exchanged is sensitive information. For activist groups these will not be significant issues, so we will not cover them further here. Many are also more useful for very small teams or where you might want to avoid any pattern or regular reaction. A professional tail will actually walk on rather than go round a corner, consider ducking into an office block and concealing yourself there; this is ideal for watching those coming in behind you, as are many walls. However, there are limits to these tools and if you take sensible precautions, especially in the setting up and using them, then even then CCTV would be hard to scale of fears (unless you are under some seriously heavy surveillance). If there are a concern, then rooms with out windows would be good, or cover sounds so as not to rouse muffled sounds. Add further problems by putting a stereo speakers next to the window.

When setting up meetings, depending on the degree of contact and geographical distance of the parties athened take the advice of PGP face to face contacts or coded postcards/birthday cards for exchanging the initial meeting place / dates.

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

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, overwroking, etc.).

If one of the parties is delayed, this allows the other par- ties to leave, turn on your phones to get a statement of how long they will be and then when they think the surveillance occurred, and then for the parties to move to the next destina- tion. Note: if there is a large time delay it is best not to go to the meeting point until the appointed time so as not to avoid hanging around and attracting attention. Finding the place and going somewhere else is wait normally okay.

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; or you are stuck with ordinary paper then do it piecemeal – putting too much at once in your mouth will give problems with swallowing it.

Directional and parabolic microphones are very power- ful theses, but will give off a buzzing noise even if someone is not nearby. However, there are limits to these tools and if you take sensible precautions, especially in the setting up and using them, then as there are many observation points available as well as exits. Balconies are ideal for watching those coming in behind you, as are shops with larger doors, balconies or windows. If you have a may get a away route through passageways to nearby buildings or car parks. Other tactics worth mentioning is to use up unused exits to get out of it. If you are staying over enter shops at the last minute when you look like you are about to leave. Standard procedure for surveillance teams is to cover all exits.

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

Active detection

• Drop some paper (make it look like it accidently falls out of your pocket as you take your hand out of it) and see if anyone takes note.

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

• The main tool for detecting foot surveillance is the blind corner. A meeting point uniting all the people to be in a place at a certain time. Note: if there is a large time delay it is best not to go to the meeting point until the appointed time so as not to give them the slip or to observe their reactions. However, a professional tail will actually walk on rather than go round the blind corner, and use their communications gear to get another member of the team pick you up.

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

• Double back on yourself, and repeat to see who you keep a watch on. If there is a café or shop with a good window see so are not prepared for, or by simply stopping and watching. If there is a café or shop with a good window see so are not prepared for, or by simply stopping and watching.

Active detection

• Drop some paper (make it look like it accidently falls out of your pocket as you take your hand out of it) and see if anyone takes note.

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

• The main tool for detecting foot surveillance is the blind corner. A meeting point uniting all the people to be in a place at a certain time. Note: if there is a large time delay it is best not to go to the meeting point until the appointed time so as not to give them the slip or to observe their reactions. However, a professional tail will actually walk on rather than go round the blind corner, and use their communications gear to get another member of the team pick you up.

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

• Double back on yourself, and repeat to see who you keep a watch on. If there is a café or shop with a good window see so are not prepared for, or by simply stopping and watching.

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

Waiting in a queue for a bus is a useful method to spot the surveillance team into thinking you are conforming, then seize an opportunity to disappear elsewhere.

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

• You can also bring changes of clothing and appearance (e.g. cut your hair). Only do this if they are cut to look good; badly fitting wigs only draw attention. As well as change of clothes have a secondHauck bag to carry them in – avoid using the same one with different clothes.

• Some quick ways to lose a tail are:
  o Dash across a busy road the moment a gap appears. Use the opportunity to disappear down side streets or into any building with alternative entrances.
  o Have a friend pull in and pick you up from a route where the surveillance team will not be following you in a vehicle. It may be that this can be done discreetly with you hiding in the back under a blanket, but you will have to make sure that you are not being followed and it and they are not familiar with the vehicle or the driver.

Getting into a crowd – a classic, but it does work.

Factories and football matches are good as this is well known, but if this sort of event is happening near you

• Shops with multiple and/or out of the way exits are good for both active surveillance detection (wait
direction. If you know the area quite well, it means you can take a route that is hard for them to pick you up again.

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

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

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

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

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

### 7.3 On foot

If you are being followed on foot again it is likely to use a team of people rather than an individual. Their dress will be nondescript and have few identifying marks or clothes. Saying that, ordinary policemen are quite easy to spot even in plain clothes though not necessarily foolproof:

- In a similar case both the shop and anyone watching as people as possible, and definitely face the door. o Keep an eye out for couples who are not chatting or not acting naturally. It has been known that while a group has been relaxing in a pub surveillance team members have come in and set next to them to prevent bags containing listening devices. They gave themselves by their body language, consuming their beer or food slowly or not at all, and have very poor interaction among themselves. Remember to look instead people from the group going to the bar or toilet, etc.
- Is there an upstairs seating area with windows overlooking the street? This is a good place to sit and watch if anyone is loitering, waiting for you. Do suspect individuals watching the door to the café, etc., regularly.
- In a bookshop is there anyone looking at the same books as you as you browse through, or are they political ones?
- On bridges and the like you can also stop to admire the view, again giving you the chance to look around you. Who looks like they do not know where they are going?
- Stairs and escalators in a shop give opportunities to look for approach from the opposite direction. So when you reach them you have to do a half circle turn, so able to look behind you without appearing to do it if you want.
- As you leave a shop, stop and ask someone the time or for directions, keep an eye on who might have followed you.
- Chose a narrow or quiet street to act as a choke point to filter suspects out from the crowds making them easier to identify. Doesn’t always work with a professional team as well as they will be prepared for this. If this is not a place you would go in the normal course of business then it is better to do your own thing.
- If in a train or bus station, change position regularly and watch those standing still. Keep an eye out for people not really looking at you and watch them properly. If purchasing a ticket, etc, watch out for people standing right behind you who may be able to overhear.
- In shops who is not actually shopping or appears out of place.
- If approach a place you plan to use as your own observation point, if the spot who is already there to eliminate them consider.
- In general do not centre of town or low on pedestrians in general do vehicles at state level points pull out and travel slowly behind you. More professional ones will move ahead of you and wait you to pass properly.
- Enter a place where an unprepared tail will look out of place, e.g. a punk shop, etc. If this is not an obvious place for you to be in then it becomes an active detection technique so hints at the fact you are watching out for surveillance.
- As you cross a street who on the other side slows down to avoid crossing your path. Do they cross to the other side but continue in the same direction as you? At a junction who quickens pace to cross it before you do?
- 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.
- If the shop has a back entrance leave through it, and
- People sitting in cars for prolonged periods at your office or home.
- You see the same faces repeatedly around your homes and offices.
- Increases in police patrols passing by.
- An increase in numbers of people being approached to be a grass.
- Regular tears in parcels.
- corners of envelops broken.
- The mail arriving late and at once.
- Mail regularly disappearing.

Remember, many of these warning signs by themselves are not sufficient to indicate that you are being monitored, but if you are experiencing one of these combined with others running a campaign threatening to be successful then the chances are you are being watched in some way.

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, so a good practice 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, or Intelligence Community, are more likely to seize equipment you need to function. Backing-up of anything valuable is important!

### 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 the 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 be the subject of discreet harassment.

- People taking photographs of the building.
- People taking down licence plates in the vicinity.
- New people attending your meetings and showing excessive interest in what is happening.
- Keen 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.
- People sitting in cars for prolonged periods at your office or home.

### 3.1 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. Infiltrators will 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 and their superficial knowledge of issue and their inappropriate dress sense.
Why would you suspect you have an infiltrator in the first place? Of a group which is not dealing with security on a day to day basis? You may know of examples where they have been identified. The main thing is to avoid letting paranoia taking over – think back to the situation to them because you’ve gone into paranoid mode will get you driven out or put off. What may seem obvious to us is only noticed joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly; it should not be mentioned joking in conversation behind someone’s back as that is being done by people who, with the group. So it is not to be done lightly;
When the culprit is signposted and your tail is professional then they will not be caught out by this, but it still often works on the average investigator or police who have not got the experience tailing people watching out for such activity.

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

In some cases they will actually stop. Further up or around the next exit point is usual. As by this time it is probable that they realise they’ve been clocked. However, if you are an experienced police officer, they will quite often wait around to do 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 take further action), easy for them a question for directions. It allows you to look at what they look like, while at the same time letting them know their cover has been blown.

Use routes that are not obvious to your destination such as taking the long way around an estate or several blockages. If you are driving too fast you will have to get close. Remember, cover stories tend to be a mix of both truth and lies. Make notes of any inconsistencies but allow for the fact that people often exaggerate anyway just to fit in. If they claim to be involved in other group, approach that one instead. If they are involved in another group this may be tricky to prove. In some cases they tail will actually come from. On a narrow cul-de-sac you can be able to react faster to keep you in sight. They may have to allow for the fact that if you come off at a junction they need to turn around, which is why the police suspect presence of the group 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 prematurity.

Discretely ask the suspect about their background and personal life and check it out. It is very hard to lie consistently over time, especially if you are probing in areas they do not have a cover prepared. Remember, cover stories tend to be a mix of both truth and lies. Make notes of any inconsistencies but allow for the fact that people often exaggerate anyway just to fit in. If they claim to be involved in other group, approach that group and maybe with a photo in case the suspect has changed their name. Often when an infiltrator has been exposed in one group, they simply move onto other ones and on roads with long range visibility and low density traffic on them they may be that they do not need to be as close. Once you are aware of this, then if the suspect is one, one surveillance vehicle, then it may be replaced by one travelling further behind it.

Who follows you into a service stop or over a junction and then back on to your original route, the police cars parked up with the entrance of the cul-de-sac in sight and who start moving once you leave the cul-de-sac. Driveways may be used as well, but may depend on high enough housing density to work.

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

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

Set a trap. “Arrange” an action or meeting that the suspect is involved in and check to see if there are any police or extra security waiting. If the subject is talking about their interaction with others in the group this may be tricky to organise. Next step to be planned correctly, and to be done to be more than once to catch the person out, espe-

ially if they are in for the long term as they will wish to avoid suspicion. As this method they have to a chance to have a chance to properly integrate with the group. Also one set of un-

planned extra presence can be explained away as bad luck; more set up it may be bad security practice on the behalf of the suspect such as talking openly over the phone about – in which case you know they are involved.

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

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

If you suspect you have an agent provocateur consider getting them to incriminate themselves – have a dicta-

phone ready so when the opportunity arises you have the evidence you need. Avoid making a scene against you in the future. Then it was the infiltrator or the grass who tried to entrap you. Keep the recordings secure (not in your house) and make backup copies. Consider talking to a lawyer you can trust.

Most police infiltrators will try to avoid being active in anything that may be construed as illegal as this will com-

promise their evidence in court – especially if it could 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 do this, and it is also illegal. It is important that you 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 strong belief that someone is attempting to set you up.

There are other problem types besides infiltrators. Some from the group will spend much time talking in an attempt in order to create a more exciting response or story, so setting up opportunities for their stories. There are also those individuals who are a bit wild and will dis-

rupt if they cannot get their way within a group, and end up destroying it out of petulance rather than deliberately creating it.

What is important is that you do not go public on insufficient evidence – what happens if you get it wrong? You could lose a person who could subsequently be turned against you, and you can destroy much of your good work and disrupt your effectiveness. People can turn on you as well.

3.4 EXPOSING THE INFILTRATOR

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

Firstly, arrange a meeting between a few of you with the suspect and put your evidence before them. Watch their reactions and carefully observe their reactions to the evidence. By the time the evidence should be sufficient for them to chuck it in—not maybe without shouting that it's all a hoax but you cannot work without conditions, etc. If you are going to expose someone subsequently, get a photograph of your infiltrator while you can.

Next, arrange a full meeting of your group, and put the case before them. It is wise not to announce the true purpose of the meeting beforehand, as if others talk to your suspect they may tip them off inadvertently. You do not want to announce any new allegations without a meeting. Any meeting etc. you will challenge the suspect shortly before the meeting. If they do come to the meeting to defend themselves, they will be better prepared and change their story to adapt to the evidence, so you will have to challenge them on this—this is the main reason for having witnesses at the initial confrontation.

At the end of the meeting, ask the suspect to leave the room to 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 circum-
spectly you need to tread more carefully. A potential approach is to confront the person with your suspicions as it may be more conducive to your group. This is to go to an anonymous member and tell them there have been sexual relations between the infiltrator and group members. Some group members will not want to hear about it, but if you have been coned in this fashion and their objections may be based on this.

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

### 3.6 Gatherings

These pose a different set of problems. However, final author-
ity normally rests with the organizers, or a sub-committee specially convened to deal with this issue, to ask the suspect to leave. You do not have much time to gather evidence, but in our experience spotting them is not particularly difficult as infiltrators do not go to significant amounts of effort to cover
their activities. Likewise with a lay-by or lay-by on a motorway or main road.

If you are aware of a blind turn or a sharp hill, drive fast into it and once through it slow down immediately. What
waits behind rather than go through?

When you take turns or side streets there is a possibility
the surveillance team will have to expose themselves with unnatural
activity. It is possible that what you are trying to avoid is what the surveillance team is trying to expose you to.

### 3.5 Dealing with the fallout

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

- Consider going to the press to highlight the issue, though this clearly depends on the nature of your group as to how appropriate it is. It is a tactic more suitable to more mainstream groups.
- Let other groups know through established channels. Publicly announce the group of the person on relevant websites and other news services (magazines, indymedia, etc) so others are able to identify the as infiltrators, that so they do not fall cannot be talked to the same individual. Be prepared to substantiate your accusations. Send a letter to all the groups you are connected with and explain what you are running to do to minimize the problem. An example of how one infiltrator was exposed and advertised is the first request from the Borderlands by Larry O'Hara, which deals with the activities of the infiltrator Tim Hepple/ Mathews.

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

- Put in processes for preventing it in the future— it can help retain your reputation, following any backlash over the exposure.
- Put in to place processes to minimise the damage to your group. This is important to stop unnecessary paranoia and inflating 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 hear about it, but if you have been coned in this fashion and their objections may be based on this.

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

- Vehicles tailing will generally drive two to four cars back. Depending on the nature of the traffic and the road, they need to keep you in sight, so watch out for vehicles pulling out of the lane to your right and then driving back in. There will be points at which they close up on you, depending on obstacles and other traffic situations, e.g., road works, traffic lights. This gives the infiltrator the chance to get a closer look at you. One bit of suspicious behaviour is when a vehicle slows prematurely so as to back your tactics and then, when they see the flow of traffic. Surveillance drivers often instinctively of pacing their driving to the target vehicle will disrupt the tail.

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

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

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

- Adverse weather conditions will cause surveillance vehicles to drive closer than they normally would due to poor visibility; in particular, in bad weather they will drive in front of the target vehicle.

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

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

- Enter a petrol station and see who else follows you in. Is there any other way to the shop but used to go to where you have been in such a place? Is this other a shop or is another car parked up?

- Ask the following questions about the suspect person:
  - When they take notes at what point do they do it?
  - Who are they watching and listening to? How keen are they on particular individuals and at writing down people's names?
  - How are they making approaches to people?
7.2 Vehicles

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

- Bad window-shopping (compare how people usually do it by moving their heads, as opposed to a tail who is trying to see in the reflection or not properly looking at all)
- The same person taking yet another phone call
- Someone in a phone-booth doing more observing than talking.
- Avoiding making eye-contact at all cost.
- General uncertainty if you break an established pattern.
- Are they carrying a video camera in it?
- Carrying out repeated scratching of head or checking of watch – possible non-verbal communication signals.
- Silhouette at night.
- Light for vehicles to see in the reflection or not properly looking at all).
- Broken lights
- Body shape
- Number plates:
  - o Memorize number plates: if you spot a car you are suspicious of, look at the number plate and turn the last three letters into a word, e.g. B0H becomes BaChAn. Words are easier to recall than numbers and letters, and if you come up with the same word, again you can turn it quicker.
  - o 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 police car. Some unmarked police cars actually have police written on their tax discs.
- Number plates:
  - o Memorize number plates: if you spot a car you are suspicious of, look at the number plate and turn the last three letters into a word, e.g. B0H becomes BaChAn. Words are easier to recall than numbers and letters, and if you come up with the same word, again you can turn it quicker.
  - o 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 police car. Some unmarked police cars actually have police written on their tax discs.
- Does the vehicle look out of place for the area you are in? It is harder to identify when out and about unless you know the area quite well. Or does the vehicle look modified. See the section on personal security for more on what to look in a vehicle parked up like this.
- As you pass identified pick-up points, watch the parked vehicle. Often they will park in the same direction as you normally take and on the same side as the flow of the traffic.
  - o Can you see maps and signs of people sitting in them for a while, e.g. coffee cups, food packets on the windows?
  - o Is possible check the exhaust to see if it is running and waiting to go.
  - o In cold weather are they getting out to clean the windows regularly?
  - o Do they pull out behind you as you pass?
4. Security for Actions

Actions come in many different forms, each with its own security needs. Many ideas mentioned under campaigns and personal security may also apply here so we will not duplicate ourselves here. But hope what is that and what is not is obvious.

4.1 Choosing people

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

4.1.1 Approaching people

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

If you ask them about doing an action and they initially say no ask about it later, unless they are expressing an interest in being involved, then tell them it has been called off. Once committed warn people against backing out later or talking about it. The degree of secrecy needs to be made clear right from the start so people are clued in otherwise there are inadvertent breaches of secrecy. Always get together in a safe place, as active are not to run self-help groups, but to make changes. That sound harsh, but so is losing your freedom because of someone else's personal or political ambitions. If someone tells you they will not be involved, keep them out of it.

4.1.2 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. If you are planning an action you are aware of and you think they are not doing it with you they can rely on if things go wrong, or can be counted on to do their part to make sure that things do not go wrong.

4.1.3 Watch out for bravado

Drug users and heavy drinkers are a liability, as are people with money-draining habits such as gambling. As well as being unreliable, they are much easier to turn or trick into talking. Remember the very famous story of the co-conspirators in the US, where a number of ELF activists were arrested up to a decade after they were involved, was by using one activist's heroin addiction to get them to talk. They were active not to run self-help groups, but to make changes. That sound harsh, but so is losing your freedom because of someone else's personal or political ambitions.

Addictions can also cause people to fail to carry out important tasks relevant to the action. If you are the leader of the action or rest of the group in jeopardy, this runs the gamut from not turning up on time to go to a hunt sab or demo to acquiring information about your PLU at the right time. Do not arrange or hint at meetings in front of those not involved as it is quite disheartening to future activists.

4.1.3.1 Watch out for bravado

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

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

4.1.4 Watch out for the boasters

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

4.1.5 High profile people

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

4.1.6 People with issues

If you are a heavy drinker, drug user, etc consider how you may be jeopardizing others so consider moderating your mental health issues where the stress of taking risks may prove to be too much, or that later on, after the action, they may not fully understand the need for maintaining security in respect to it.

When a surveillance team loses sight of their target they will attempt to find you as opposed to giving up. The first thing they do is search the surrounding side roads or alleys to see if they have turned down any. If they fail to find you they will return to where they lost you and continue in the same direction as you were last known to be travelling, with specific. A good network of activists always follow the vehicles following them you may have not spotted them all and you could simply be picking up another one of the team.

If evasion is not an issue then it does not matter that they are police then they will give up attempting to be covert, and simply follow you overtly.

Exposure

Surveillance operatives are desperate to avoid exposure, but it takes them a particularly skilled operative to avoid doing so. If a team is working on you they will have only one operative or vehicle exposed to your observation.

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

It is also worth allowing patterns to be established as this lulls them in to complacency and dropping their guard slightly – surveillance is hard to keep up for a prolonged time at the same level of intensity. Thus, when you break the pattern, they are more likely to show their surprise. When you are traveling a route other than the one you are following, you may be automatically more alert to your actions.

7.1.2 What to watch out for

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

Can you see them repeatedly pressing buttons on a radio as they talk? Are they talking repeatedly and peering forward? While on foot when a suspect vehicle passes you does it speed up as it passes; does it quickly turn down a side street?

Exposure

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

• Coupling, tripping and other behaviours of someone who is being distracted when there is no obvious reason.

• Signs of tensions such as pacing, frowning staring, checking the time repeatedly, twitching.

• General awkward mannerisms.

• Speaking into collars or their chin lowered into their chests as they speak.

• Touching their ears repeatedly is instinctive reaction to an eavesdropping voice.

• Is there a wire running down to their collar? Though with the prevalence of personal stereos and mp3 player this is far more common place and harder to spot. They may be parked a few blocks out of place with the rest of the person's attire.

• Do they stop and stare into nothing – a feature of someone taking a message.
A less obvious risk are people who have personal reasons for joining a group and are not necessarily motivated entirely by the aims of the movement. They may consider activists as cool people, and so by being involved in the organisation, they may presents themselves as a part of it, even if they are not.

4.1.7 Security and your affinity group

The final point when bringing your team or affinity group together is to ensure that everyone is working to the same standard. This can be done by having an awareness that some people are not doing enough to keep the group secure and others are being too paranoid to the point it is disruptive or disempowering. Discuss it through and make sure that everyone knows what security measures they have to take and why. As in campaign security, it is best to reach a consensus whereby everyone is clued in to the needs of the situation and acts appropriately. Such discussions are also a good way to spot people who are only giving lip-sync to the requests or being too blase 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 pushed up into the team and simple. A classic case of this is mobile phones at gatherings. If the group decision is that mobile phones have batteries removed and not taken to meetings, and that people do not make phone calls at gatherings. If the group decision is that mobile phones have batteries removed and not taken to meetings, and that people do not make phone calls.
Often actions may involve known activists from elsewhere. This is not always possible to avoid but you should try to get a meeting around your social group or at a social event before letting them in on who else is involved. Avoid organisings if someone is doing the organising, they should meet with you. Setting up a meeting is ideally done face-to-face. It is bad to forget to burn it later so you end up carrying it around with you. Tip: always carry a lighter so you can light it on a piece of paper. Tip: avoid using obscure, half-broken sentences. Phrases such as ‘I have been up to no good’ or that will tip the authorities to the fact that you are a political activist. Basically, do not say anything on the phone or by email that will help to compromise you. If there are several parts to an action, not everyone needs to know about 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 draw connections between individuals. Do not suddenly have an influx of visitors coming to your house and doing the same thing when the police come snooping. Also with this, if you are being watched, they have probably already been seen at it for several days and you are being watched. It will not be hard for them to move up to more sophisticated methods while you are still trying to identify the surveillance team. Surveillance will take place over many days so it is useful to keep what you’ve noticed in mind (or make a note to remind you). For example, if the same face or vehicle does appear again at a later stage.

Similarly, you need to beware of being unnecessarily paranoid when it comes to detecting surveillance. A suspicion that you have been seen or are under surveillance, where none is in fact present, is definitely not a good idea. The longer the gap between pur- chasing and using equipment was purchased and hence maybe to CCTV implications. Buy materials and hire vehicles well out of your area. Be prepared to put a lot of planning and thought into this. Avoid using your own vehicle if there is that option. If you have hired a vehicle, do not park it near your house. Where possible avoid using credit cards, though it is often hard to hire vehicles with out one.

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

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

Wear a baseball cap and non-distinctive clothes when making purchases; consider buying a set of clothes from a charity shop and once all your purchases are made dispose of them. It is best to dress down and blend in – wearing radical T-Shirts is the person or vehicle under surveillance. If a surveillance team member or vehicle is visible to you first familiarise yourself with the following glossary:

- Target Pattern Analysis: if a surveillance team member or vehicle is visible to you, you can identify surveillance by using a specific technique that allows you to identify the target accurately. This technique involves observing the target’s movements and identifying any unusual or suspicious activity. The goal is to detect surveillance as early as possible, so you can take appropriate action to prevent it from happening in the first place. Surveillance techniques used by law enforcement agencies can be categorized into three main types:
  - Physical Surveillance: Physical surveillance involves the use of human agents to observe and monitor the target. This type of surveillance is usually conducted using teams of agents who are trained to detect suspicious activity and report it to authorities.
  - Electronic Surveillance: Electronic surveillance involves the use of technology to monitor the target. This type of surveillance can include the use of cameras, microphones, and other electronic devices to gather information on the target.
  - Financial Surveillance: Financial surveillance involves the use of financial records to monitor the target. This type of surveillance is usually conducted by analyzing financial records and identifying any unusual or suspicious transactions.

- Active Surveillance: Active surveillance involves taking positive steps to identify and disrupt surveillance. This type of surveillance is usually conducted using teams of agents who are trained to detect surveillance and take appropriate action to prevent it from happening. Active surveillance techniques are often used by law enforcement agencies to prevent terrorism and other criminal activity.
7. Surveillance

Being put under surveillance is a fact of life for the political ac-
ivist. It is actually a sign that you are being taken seriously so it
is not always something to be concerned about. It is certainly
not being paranoid for humans, as it does, and much more regular than is supposed, though not often in a
systematic manner. There is no basic right that stops you from
being the target. Being followed by professionals is very hard to
prevent, as it is rare for just one car to be used. In

order to deter rather than arrest.

as they are too visible to get away with it, and their aim is often
lost or being observed. Many police now simply follow openly
in the UK. Imprints of footwear can now be taken at the
environment.

Tip

4.6.4 Fingerprints

and gloves.

4.6.3 Hair

The alternative of providing the forensics team with no infor-
mation at all is to provide them with too much information
due to pretty convincing evidence. Markings can be as simple as a
surface you touch, including palm prints – forensics look at
markings on shoes and used to identify your shoes as the

For a good intro-
to DNA forensics check out the GeneWatch report at:
http://www.genewatch.org/HumanGen/Publications/Brief

ports/NationalDNADatabase.pdf

4.6.1 Footwear

Shoes and other footwear all leave distinctive marks; cuts and
wearing in the treads can be used to identify your shoes as the
ones leaving a trail. This is an issue if you are going to be in an
area with mud or you have to cross it. Buy disposable pairs or
put socks (which will pull up high) over the top of them, with
a plastic bag between the outer sock and the footwear, so when
you come to take the muddy socks off, you can do it in a clean
and bag up the mud and dirty outer socks in one go
without getting it on your hands or clothes.

Tip: If in the field always plan in case of getting mud on
the rest of your clothes, especially your trousers. If you have to
leg it as part of a getaway it may alone you into a
town or city. If stopped on the way out, an old trick was for everyone to take
off the mud on their shoes to the entrance of the action, so no stray hairs fall out.

Wear 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

4.6.5 Maps

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

Techniques to use with maps are

• Do not use markings that cannot be easily erased – this
goes for pencils which leave indentations even after being erased.

• Use laminated maps where tell-tale marks can be wiped
quickly and more securely and don’t have as big an issue

• If in doubt, buy new ones with easy wipe covers and use
gloves.

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

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

Clothes can be used to disguise your shape as well, so go

for baggy clothes which create an asexual figure.

• Keep your hair and facial features hidden. Hoodies and base-
caps are good, as are masks and balacivas. However this
depends on the situation, as sometimes wearing masks and
caps is too noticeable. Many activists are good as they can be quite
obscuring, and they are a legitimate clothing item. Ski masks are not as good as
they can give away too much facial features around the

16
of 45

black is not always the best colour, for instance getting
caught in a field of snow. Consider grey or khaki. In our

16
of 45

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

4.6.5 Maps

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

Techniques to use with maps are

• Do not use markings that cannot be easily erased – this
goes for pencils which leave indentations even after being erased.

• Use laminated maps where tell-tale marks can be wiped
quickly and more securely and don’t have as big an issue

• If in doubt, buy new ones with easy wipe covers and use
gloves.

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

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

Clothes can be used to disguise your shape as well, so go

for baggy clothes which create an asexual figure.

• Keep your hair and facial features hidden. Hoodies and base-
caps are good, as are masks and balacivas. However this
depends on the situation, as sometimes wearing masks and
caps is too noticeable. Many activists are good as they can be quite
obscuring, and they are a legitimate clothing item. Ski masks are not as good as
they can give away too much facial features around the

16
of 45
4.6.5 Other materials
It is a good policy to remove any unnecessary items from your clothes before you leave to go on the action. Anything that can fall out of your pocket could end up being traced to you through forensics. Don’t forget things that rattle, etc. take only the keys you need and not the full key ring. Though bring some change for phone calls.

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

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

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

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

There are reasons for this. Even if they trace the vehicle, you don’t want to leave markings in it that may be used against you, or leave anything that could be found that would leave memories of mud, etc. in the mind of the rental company.

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

4.7 DISPOSING OF EQUIPMENT/CLOTHES
This is something you should budget time and preparation for. It is often forgotten about, but is crucial as it ties up with your action.

Anything that may compromise you should be burned or otherwise securely disposed of. Dumping them in a river/bin a few miles away may not be enough. The more you leave at the scene of 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, but it is still their right to know about it for handling. They are not hard to set up so are also useful for surveillance – keep regularly changing ownership of the vehicle. Generally you can do this as often as you want. In the UK a vehicle can only be registered to a PO Box if it is in the name of a registered business. The State, as a rule, is very keen on who drives vehicles are, as to their way of thinking it is a position indicative of a leadership role and as useful people to take in order to cripple a group.

6.5 Self Defence
Security includes also protecting yourself from physical harm. When out and about being active you never know what sort of security guards, hunters, etc. Learning a few basic moves on self-defence courses will teach you what you need to know in order to get away is important. Security also includes protecting yourself from physical harm. When out and about being active you never know what sort of security guards, hunters, etc. Learning a few basic moves on self-defence courses will teach you what you need to know.

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

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

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

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

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

If the need is over for the phone to be taken out, be absolutely sure of disposing properly of any up and put a long ranged directional microphone in its direction, which can pick up on conversations through walls.

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

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

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

If you are friendly with neighbours, then you can pick up on people approaching them to ask questions about you, and if it seems all right to talk both or believe your explanation then do they 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 by watching the 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 light in them, or curtains that never shut fully. What 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 a meeting shouldn’t be you will be able to recognize the fact straight away. This is not common, but has occasionally happened.

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

One final tip for your neighbourhood is to get to know your es- tate quite well. Watch out for cars being parked up in unusual places shortly before you go on the action and at the end of your road can be a sign 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 be watching you and might be taking up 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 what is happening. What has been found useful by some is when checking if they have a potential tail, watch for being parked at a shop, use materials if 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 by itself, but it is worth noting the cars making, colour and number plates so that if it appears later it can be immediately clocked as a tail. If you strongly suspect a van or car is being used for surveillance on you, stop to tie your shoelace next to it and have a good look at it:

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

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

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

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

6.5 Self Defence
Security includes also protecting yourself from physical harm. When out and about being active you never know what sort of security guards, hunters, etc. Learning a few basic moves on self-defence courses will teach you what you need to know.
do test runs to ensure they work properly and do not give false positives.

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

Alarm systems 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 not expecting people you do not have to stuff some 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 intrusions during a raid can put bugs in your house. This is why you should never say anything you would feel uncomfortable about defending in court, that would give away plans for actions, or would implicate yourself and others. Or indeed gossip that could be used against you.

Bugs come in a variety of different forms and sizes and can be highly sophisticated. Most are now voice activated and designed to blend into any type of music on the radio. Be aware that while they may not necessarily be effective against them. As well as breaking in, other ways of getting bugs into your house (or office) is through ‘guests’, new appliances which have been intercepted, and gifts. Some offices have a policy of meeting people away from the office. In an effort to blend in well. Old tricks such as running water and conversations, or would implicate yourself and others. Or indeed gossip about defending in court, that would give away plans for action. 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 increased the frequency to 3GHz. The real high-tech scanners cost in the tens of thousands of pounds and require professionals to operate. However, police and other investigator may rely on older equipment depending on their own budget constraints.

On one hand, many people still use bugs that can be found by over-the-counter detectors so they can be found. On the other hand, it can lead to a false sense of security, and in fact bugs can encourage the surveillance people to use more effective techniques. If one does find bugs your other security precautions will be of little use. Another of the bugs is that they are out of sight and easy to put in.

On a personal note, being bugged is disgusting. It does feel like an invasion of privacy. However, if you are mentally prepared to use it for that purpose and are taking sensible precautions then the bug won’t have any effect. However, if you have any questions as to what they are actually hearing? Then your thinking it to be one that should you and you friends. While you will need to be one step ahead of the bugs themselves. When bug detecting equipment to do test runs to ensure they work properly and do not give false positives.

It may not be transmitting at the time you are scanning. It may not be transmitting at the time you are scanning. When bug detecting equipment to do test runs to ensure they work properly and do not give false positives.

6.2.5.2 Your Car, the Garden & the Environments

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 in woodland woods and parks. All these have been known to be bugged. It is often worth checking them – especially if your car. Similarly phone boxes in your immediate vicinity. In the UK it is possible to type in 141 before dialling the number.

When driving, pick country roads and motorways, avoiding towns as much as possible- as that is where the greatest concentration may be. Be aware that vehicles are not as likely to be monitored as it is 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.

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

Avoid areas were you are likely to be already monitored, such as town centres where there is already much CCTV or areas with heavy traffic. A simple bug scanner may often pick up if there is a camera monitoring it by picking up on the camera’s transmissions back to base.

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

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

Phone box to phone box calls are not secure; in fact they are seen as a trigger for state monitoring. However, for many numbers, especially those not commonly targeted it will still work.

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

6.10 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 this we suggest the following guidelines:

• 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.

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

• Avoid areas where you are likely to be already monitored, such as town centres where there is already much CCTV or areas with heavy traffic. A simple bug scanner may often pick up if there is a camera monitoring it by picking up on the camera’s transmissions back to base.

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

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

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

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

In the UK it is possible to type in 141 before dialling the number.

4.11 cctv

CCTV is everywhere these days, but not impossible to hide. 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.

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.

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.

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.

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.
4.13.1 On foot

Scatter in groups of between two and three, preferably matched by speed. Do not walk straight, wait until someone chooses the alley you are to follow, and then change direction with a smooth turn. If you are being watched closely, it may be worth trying to lose it. However difficult it is, keep your cool until you are certain that the police are on you – more often than not it has been possible to talk your way out of it.

4.13.1.1 In the car

The car will, however, get rid of DNA evidence. Practically, never say anything on the phone you would not be prepared to stand up in court and admit. Never plan anything remotely incriminating to match the replacement number plates from a similar make and colour of car to the ones used on actions, so automatic number plate recognition monitoring does not trigger any alerts (eg wrong type of car or non-existing number plate. However, one must be aware that it will not defeat bugs in your phone or computer. If a number-plate is recognised as belonging to a stolen vehicle or a car belonging to a known activist, then the police may stop the vehicle. Currently these cameras are mounted in police vehicles. However, the Government is currently rolling out a scheme to convert traffic camera to have ANPR with the data being passed to a database control stations and supermarkets are also being brought into this network. This will allow them to record every vehicle which will allow them to analyse journeys made over several years if necessary. More information on this is at http://news.independent.co.uk/uk/transport/article334688.ece

4.13.2 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. Remember even experienced activists in case that it is not clear how covert the action is to be. If you are reminded to use a payphone or clean phone, you should use it. Remember, the phone and email are useful for facilitating and coordinating actions but they do have their limitations. For example, it is impossible to replace (unless they clear up the mess and start again) if you have broadband, to make phone calls, which allow them to sometimes check up these cover stories. The best advice is to avoid anything in letters that either incriminates yourself or others.

If you are certain that it is the police and not others who are sensitive to the fact that you are on to them, it may be worth trying to lose it. However difficult it is, keep your cool until you are certain that the police are on you – more often than not it has been possible to talk your way out of it. Just so you know.

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 inform the police so that they do not stop people behind blundering into situations and reduce the ease of being spotted. Keep your attention on moving and not discussing what went right/wrong.

Different groups should move in different directions; you do not want to be leading the police to another group of you. When doing preparation for an action run through the route to the rendezvous point (after you have spoken to them). It will usually make it so knows of any issues not identifiable on maps or of other dangers.

Always have a secondary rendezvous and time in case this is not possible. In this case the police will have obtained maps (no markings) and/or be familiar with where they are and what they are looking for. There should also be a time limit on how they are likely to go to this amount of trouble unless they are pretty determined to get the activists, and even then it may simply lead to a waste of police time. Burning out the car will, however, get rid of DNA evidence.

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

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 grubbed 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, it is always best to avoid the possibility of police actions being used (though unfortunately not always), such visits are simply to rattle and intimidate you; as such they should be treated more as a statement about the level of their intelligence and the evidence they had. If their intelligence was particularly good then you would be dropping both more false implications that you are guilty, but dragging you to the police station for a less friendly one.

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

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. Remember even experienced activists in case that it is not clear how covert the action is to be. If you are reminded to use a payphone or clean phone, you should use it. Remember, the phone and email are useful for facilitating and coordinating actions but they do have their limitations. For example, it is impossible to replace (unless they clear up the mess and start again) if you have broadband, to make phone calls, which allow them to sometimes check up these cover stories. The best advice is to avoid anything in letters that either incriminates yourself or others.

A new technique is being rolled out by a number-plate tracking device. This will allow them to record every vehicle which will allow them to analyse journeys made over several years if necessary. More information on this is at http://news.independent.co.uk/uk/transport/article334688.ece
member of society. It is all very well to debate the nature of what is 'everyday' and 'normality', but the reality for a covert activist is that the stereotypes are generally quite clear; these debates should be put aside for the practical reality. Your aim is to go away and continue being active, not bringing attention to yourself but to your cause.

A person with a green mohican is very easy to follow around. Even wearing a distinctive jacket everyday is enough to mark you, especially if your target happens to be mentioned in it. Keeping a good hiding place, you can be sure that you are not going to know.

Saying that, if it is a raid by low-level coppers then there is a good chance they will look over 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 caught against the people 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 successfully manage to get hold of the disk.

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

6.2.1 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 any panic attack will be noted, so bringing further attention to 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 a lot of scrutiny, and may indicate other people as being worthy of attention.

Sensitive material should be removed from your house on a regular basis in a calm manner – not furiously. This does not prevent you from practising counter-surveillance techniques, but do change things. 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 clipping from Greenpeace can and will be produced as evidence to show that you are involved in an anti-GM issue and the inference 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 is most applicable in every situation. Work out what your security needs are and what applies to you and your actions. For example, if you are organising a straightforward demo, you do not have that much to worry about. It is consequential, consider about making life as difficult as possible for anyone investigating, but not to the point where the demo becomes impractical. For example, you don’t need to set up closed phone networks for a demo which just wastes time in the works by using unregistered mobile phones or payphones.

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

6.14 Evidence gathering tools
Directional microphones can pick up conversations even if a thousand miles away, so avoid discussing things on demonstration or when discussing issues of a highly sensitive nature, take great care of where you do it, if this sort of surveillance is a risk.

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

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

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

• With what went wrong, consider where there are people now at risk and what can be done. It should not be possible or useful to expect everyone to make the fall in solidarity with one another, if you can ensure or get them to do this, it is important to arrange support for those potentially taking a fall so they are not left feeling isolated and which could leave them vulnerable to breaking or dropping out of the movement.

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

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

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

It is useful advice but it needs some interpretation. Basically it is not about bringing attention to yourself on several levels. One level is to just not do much, destroy your house, leave your house to it to be ignored, 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.

On another level, it refers to actions with significant consequences and which may even lead to raids. Action with these sorts of risks should not be carried out near where you live. Yes, it may be possible for actions to wear only a t-shirt and go into 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 factory with a red and yellow flag, I doubt the police will kick 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 have to make value judgements and go ahead with the risks. People have got away with surprising amounts of stuff related to activism by taking by the right precautions; however, as a rule of thumb:

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

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

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

5. Security for demonstrations
If you are a person involved in covert activity consider whether attending public protests is necessary, since you want to be bringing as little attention to yourself as possible. Demonstrations are fluid things and it is impossible to guaran- tee 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 a lot of pressure to split the group because one section felt unimportant and are not about to deal with the actions of another section.

5.1 General rules for demonstrations:
• Avoid calling out peoples names; use pre-arranged nicknames or generic shouts.
5.3 Travelling to demonstrations

If a car is stopped the way to or from a protest, look away from hidden faces. If passing a police vehicle, duck down so they do not know what it is or that it is a car, but beware of the look out for vehicles packed with young people to stop and search. However, with an increased use of automatic number plate recognition technology in the UK, there is a tendency to focus on known activists' vehicles. If the vehicle you are in is regularly gone on protests then it is far more likely to be stopped. Likewise, consider if putting up posters on your car windows whether it will be drawing unnecessary attention to it, especially if they are left up while the car is parked. This is not to say don’t do it, but if you are up to something you do not want to be drawing attention to or are in a vehicle with an increased chance of being stopped, then do not make yourself too obvious.

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

5.4 Debriefing

If a protest does not go as planned and there is a heavy-handed reaction from the authorities, it is good for people to debrief afterwards, even if it is only in the affinity groups where it can help people understand each other’s reactions. This is important psychologically, and for being able to work together to a better future. Similar events happening within a group can provide them with psychological effects that find release in drugs and alcohol consumption or depression if not dealt with by discussion.

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

5.5 First Aid

The state and other opponents can resort to violence, so it important that there are people around with first aid training. These volunteers offering first aid are just as likely to say they’re coming, but not at the cost of someone’s freedom. Always respect requests to stop using camera, and never assume that you have to do so if it is an automatic requirement. Do not ask first.

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

5.6 Dealing with Provocateurs

If you see someone inflicting a situation beyond where you are willing to go, then get out of there. If you are confident that someone is provocateur then call them out with fellow activists and work out ways of dealing with it. Is good to remember that you are being battered and under surveillance, therefore you have been successful and being successful is what counts. Also if you play it right it is possible to outwit them.

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

A mistake well known activists can make is to disappear suddenly from the scene, while remaining in contact with other activists. Make sure that your alarm bell’s ring, doing a bit of background research to find out more about you for the future.

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 go to the trouble of checking who 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 alarm bell’s ring, doing a bit of background research to find out more about you for the future.

Another reason for carrying out surveillance is to confirm in formation that they have received from other sources, such as from the rest of society in stereotyping on how people dress. 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 provocateur then call them out with fellow activists and work out ways of dealing with it. Is good to remember that you are being battered and under surveillance, therefore you have been successful and being successful is what counts. Also if you play it right it is possible to outwit them.