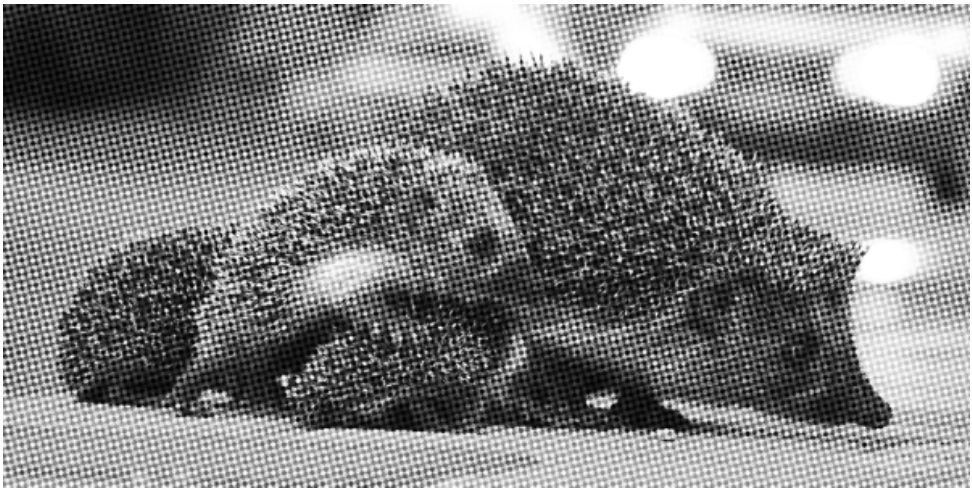
A Practical Security Handbook

No Trace Project edition



Related resource: A Practical Security Handbook for Activists and Campaigns (notrace.how/resources/#security-handbook)

A Practical Security Handbook: No Trace Project edition

Original text in English
A Practical Security Handbook for Activists and Campaigns
ActivistSecurity.org collective
2004

New edition
No Trace Project
2025

Layout
No Trace Project
notrace.how/resources/#security-handbook-2

Note from the No Trace Project:

A Practical Security Handbook for Activists and Campaigns was originally published in the United Kingdom in 2004. While part of this handbook is now outdated, we believe some of it is still very relevant.

This document is a partial re-edition of the original handbook. We have freely adapted its contents, leaving out sections that we deemed outdated or irrelevant to this re-edition, improving wording, and changing a few details, while trying to stay as close as possible to the spirit of the original text. We have also added footnotes to point the reader to up-to-date information on DNA, CCTV, and other topics.

This re-edition contains a wealth of information to help anarchists and other rebels analyze their security needs, plan and carry out direct actions, and detect or evade physical surveillance. We hope it will help you defeat the State and achieve your goals. Good luck!

The full original handbook can be found on our website.[1]

[1] https://notrace.how/resources/#security-handbook

Contents

What is security?

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

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

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

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

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

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

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

Security = Time + Effort

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

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

Setting up the "Security Process"

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

As a simple example, sending an anonymous email—you don't want it being traced back to you, so the security process is to use a dedicated email address that you create and access through Tor. You are not making yourself paranoid over the fact that they might trace the email back to you and not sending the email in the first place, but you are setting up a process which facilitates your action of sending the email securely.

Using a dedicated address to send one email is awkward and slows the whole process; however if you do not put in this extra time and effort then it is possible the email could be traced back to you, and depending on the contents it could mean you losing a lot more time…

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

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

Keep in mind that the State/corporations are not all-powerful though it may appear so (they encourage this belief themselves). They are restricted by budgets and simple manpower, or even infighting. They also have poor understanding about how activist groups work, and just because one part

of the organization has a good picture of your setup or access to the latest equipment, it does not mean that it is true of the rest.

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

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

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

Fortunately for us, their resources are rarely used for more than cursory work unless a political decision is made to focus on a group in particular. The less you can show your head above the parapet and attract attention

to yourself the better. An example of this which we will cover later is all the photographing at demos—they are not taking photos of you but who you are talking to or have travelled with.

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

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

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

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

Security for actions

Actions come in many different forms, each one with its own security needs. In this document we mean by actions a wide variety of events and deeds. Not all tips will be applicable to every situation, but we hope that what is and what is not will be obvious.

Choosing people

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

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 should 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 but ask about it later, then unless they are expressing an interest in being involved, tell them it has been called off. Once people are committed warn them against backing out later or talking about it. The degree of secrecy needs to be made clear right from the start so people are clued in otherwise there are inadvertent breaches of security made early on. As someone putting together an action you should NEVER assume everyone automatically has a clear idea of the level of security needed—it is up to you to remind them.

Gradually introduce people

It is best not to throw people in at the deep end, unless you are very confident in your action and in them. It is better to work them up the

ladder, watching how they react in different situations, how well they keep their cool, etc. Sometimes people make out to be more confident and skilled than they actually are. The problems will not become apparent until they are actually in action, by which point it may be too late.

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

Watch out for bravado

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

If you suspect that someone is more boasting than action, then check out if they've actually done the stuff they've claimed (e.g., wheat pasting, graffiti, etc.)

Watch out for boasters

Like with bravado, these people can be a risk. It is hard for them to not tell people about what they are up to before and after an action, even after they have been warned to secrecy—some become smug and extra secretive, which can be little better than giving away that they have something to hide. So when introducing people into your affinity group note their ability to keep secrets as they become involved more deeply. At the end

of the day our main reason for being active is to achieve social change or save lives, not to make people feel better.

High profile people

Some people are naturally under a lot of attention, whether by police or otherwise. This may be due to their apparent organizational role or simply their history of being arrested (especially for serious offenses). Even though they may be 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.

People with issues

Although we strive to be inclusive and bring many people into our movements, it does not mean everyone is suitable for every action you plan. If you are going to take risks then you have to be doing it with people you can rely on if things do go wrong, or can be counted on to do their part to make sure that things do not go wrong in the first place. We are active not to run self-help groups, but to make changes. That may sound harsh, but so is losing your freedom because of someone else's personal issues which they were unable to put aside.

Drug users and heavy drinkers can be a liability, as are people with money-draining habits such as gambling. As well as being unreliable, they can be much easier to turn or trick into talking. Recently, much of the "Green Scare" in the US, where large numbers of Earth Liberation Front activists were arrested up to a decade after they were involved, was by using one activist's heroin addiction to break him and use him to leapfrog into the rest of the groups and to entrap people by talking about what they had done years previously.[2]

Addictions can also cause people to fail to carry out important tasks properly and lie to cover up their mistakes, thus putting the action or

[2] *No Trace Project (N.T.P.) note:* For more information on this episode of repression, see the 2008 zine Green Scared?.[a]

[a] https://notrace.how/resources/#green-scared

rest of the group in jeopardy. This ranges from not turning up on time to go to a hunt sabotage or demo to failing to acquire equipment and be in place at the right time on a covert action. Another problem is when people get argumentative at unsuitable times such as on the way to an action, jeopardizing the morale and energy of the group, and whether the action itself goes ahead. This can apply to people with addictions or mental health issues.

We would also recommend against bringing along people for whom the stress of taking risks may prove too much, or who later on, after the action, may not fully understand the need for maintaining security in respect to it.

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

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

Security and your affinity group

The final point when bringing your team or affinity group together is to ensure that everyone is working to the same standards. Differing standards may mean that some people are not doing enough to keep the group secure and others are being too paranoid to the point it is disruptive or disempowering. Discuss it through and make sure that everyone knows what security measures they have to take and why. It is best to reach a consensus whereby everyone is clued in to the needs of the situation and

acts appropriately. Such discussions are also a good way to spot people who are only giving lip-sync to the requests or being too blasé about security.

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

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

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

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

Scouting out the area

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

Plan any surveillance carefully, and pay attention to the times you will be going in and out of the area. If doing walk/drive-bys do not do it so much that your face becomes recognizable, that if the police show someone a photo of you they would be able to identify you. Don't forget to use surveillance detection and anti-surveillance techniques to ensure you are not being watched yourself, thus compromising the action and its participants (these techniques are addressed later in this document).

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

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

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

Some useful techniques are to:

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

Planning

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

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

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

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

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

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

Tip 2: If people are traveling to the area by public transport to be picked up, don't pick the nearest stop or station to your house or to the place of

the action; where possible do the one before at least, so there is a bit of distance between them.

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

Communications

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

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

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

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

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

Tip: Sometimes discussion comes up during the action; be ready to deal with it, especially as important points may need to be clarified. To help with this, have a drawing board from a children's toy store in the car; it looks innocuous so helps detract from any impressions you may be up to no good, and it is also a good way of passing messages to each other that can be easily erased in one quick go (do not use permanent markers!).

Meetings

Some tips:

- Don't use a bar, especially ones commonly frequented by other activists.
- Sometimes cafes and bars are the only practical venues for a meeting.
    - If this is the situation, keep an eye on the actions of the other customers around you. Booths are not necessarily the best place if you cannot see those sitting around you, but it will depend on the venue.
    - Watch for out of place clothes or behavior, e.g. not actually drinking the beer they've bought or not properly paying attention to what they appear to be focusing on. Amateurs are easily spotted, while professionals will not even look in your direction. If in doubt, move to see if you can cause a reaction.
    - Have a story ready in case someone does chance upon your meeting. Even if that person is an activist avoid referring to the person you were meeting as an activist, or something else which would alert them that the reason the pair of you were together

was anything other than innocuous. Having your lie ready means you do not slip up. Turn the conversation away to something else as soon as possible without being too obvious about it (look for related topics and not ones completely different). Avoid fidgeting and rushing off.

- Vary the meeting places and times. Avoid doing the same place twice or otherwise creating a pattern.
- If you arrive at different times, do not hang around waiting to meet up outside before going in—it makes it obvious that you are having a meeting.
- Avoid open spaces and parks in city centers. Ideally you want a place where other people sitting or moving in circles would look out of place.
- The most secure way to arrange a meeting is by word of mouth (not over the phone/text/email), to assemble at a point, and move on from there to somewhere secure, such as the middle of a forest. This gives an opportunity for any tails to be identified and lost. Meeting points should not be railway stations, service stations or other places covered with CCTV which can be used to show that you gathered together. Don't over complicate things as that leads to mistakes. Initial meeting points should either be known to the various parties or else easy to find.
- If there are a number of you, have one of you go off and see how far your voices carry. This is particularly useful for when you are in a public venue such as a bar, where you might not have complete control over visibility.
- If your group has regular meetings, arranging to meet immediately afterwards to discuss something more serious is not a good idea; it looks more obvious than you would think, and it is harder to shake off hangers on. Very private meetings should be kept separate, though the public meetings may be an opportunity to invite people to the private meetings by writing on a piece of paper (to be burnt afterwards).
- Don't bring phones to the meeting.
- Punctuality is important; however if surveillance is spotted and the meeting is sensitive then do not attend even to warn the others as you may be letting those following you know who it is you are meeting.

- Future meetings should be planned at this meeting if possible, and not left until later. Preferably do this by passing around the details on paper.
- Even at very secure meeting points, one should still be careful.
    - Very sensitive stuff can be written down as opposed to spoken out loud. If you are using paper, first make sure you have a lighter to burn it after you are finished, but before you leave the meeting place.
    - Other materials you can use are drawing boards for ease of destroying the writing if disturbed; or use rice paper which can be eaten much more easily than ordinary paper. If you are stuck with having to eat ordinary paper, do it piecemeal—putting too much at once in your mouth will make it hard to swallow it.
    - Directional and laser microphones are very powerful these days and are able to capture audio even through some walls. However, there are limits to these tools and if you take sensible precautions, especially in setting up of the meeting, then these should be very low on your scale of fears (unless you are under some seriously heavy surveillance). If they are a concern, then rooms without windows are good, or cover windows with heavy drapes to muffle sounds. Add further problems by putting stereo speakers next to the window.
- When setting up meetings, depending on the degree of covertness and geographical distance between the people attending then consider using PGP or face to face contacts for exchanging the initial meeting place / dates.
- Take care not to give away a meeting place by scouting it out too much (the same goes for action sites).
- Consider having backup meeting places in case of unforeseen circumstances such as travel delays or a compromise of the original meeting place (because of police, overcrowding, etc.) In case this happens, all parties can meet at the backup place. Note: it is best not to go to the backup place until the appointed time so as to avoid hanging around and attracting attention. Finding the place and going somewhere else to wait is usually okay.

Acquiring equipment

Buy materials and rent vehicles well out of your area. Be prepared to have to put time and money into this. Avoid using your own vehicle if there is that option. If you have rented a vehicle, do not park it near your house. Where possible avoid using credit cards, though it is often hard to rent vehicles without one.[3]

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

Burn packaging, receipts and other such materials that may link you to the equipment and which are not necessary to keep. If there are serial numbers, etc, consider erasing or removing them, 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 the purchase.

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

---

[3] *N.T.P. note:* In many contexts, surveillance cameras and automated license plate readers are now widespread along roads, including country roads, and vehicle rental agencies routinely track their vehicles in real time. Because of this, it can be very difficult to use a vehicle without it being linked to your identity, and we generally do not recommend using a vehicle for a covert action, unless you are able to steal one in a secure way. If possible consider alternative modes of transportation such as using a bike.[a]

[a] https://notrace.how/threat-library/mitigations/transportation-by-bike.html

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

Stuff for the action should be handled with gloves and cleaned of DNA if necessary.[4]

Clothing & other traceables

During the action itself, you will leave a number of traces behind that forensics can use to investigate.[5]

Footwear

Shoes and other footwear all leave distinctive marks; cuts and wear patterns 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 such an area. Buy disposable pairs or put on socks (which pull up high) on top of the shoes, with a plastic bag between the outer sock and the footwear, so when you come to take the muddy socks off, you can do it in a clean sweep and bag up the mud and dirty outer socks in one go without getting it on your hands or clothes.

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

---

[4] *N.T.P. note:* For more information on DNA, on not contaminating action materials to begin with, and on cleaning them of DNA if necessary, see DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces.[a]

[a] https://notrace.how/resources/#dna-you-say

[5] *N.T.P. note:* For information on forensic traces, see our Threat Library's entries on DNA,[a] trace evidence[b] and fingerprints.[c]

[a] https://notrace.how/threat-library/techniques/forensics/dna.html

[b] https://notrace.how/threat-library/techniques/forensics/trace-evidence.html

[c] https://notrace.how/threat-library/techniques/forensics/fingerprints.html

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

If they are muddy, wash them off if possible, and have newspapers down in the vehicle to protect it from the mud.

Notes:

- In the United Kingdom footwear impressions can now be taken at the roadside by the police during car searches.
- Glass shards are another tell-tale sign when present on shoes and can be used to place you at a scene.

Clothes

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

Some tips:

- Black is not always the best color, for instance if you operate in a snowy environment. Consider gray or khaki. In our experience charcoal gray works best in general for not standing out in a field, etc.
- Avoid clothes made of nylon (very noisy when you move) but go for clothes that are lightweight and comfortable as a general rule—often the adrenaline rush will keep you warm, but consider if there will be much waiting around to do.
- 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 colored 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 androgynous figure.
- Keep your hair and facial features hidden. Hoods & baseball caps are good, as are masks and balaclavas. However this depends on the situation, as sometimes wearing masks and balaclavas is just too much of a give-away. Snoods are good as they can be quite obscuring, and they are a legitimate clothing item. Ski masks are not as good as they can give away too much facial features around the eyes. Covid masks can partially conceal your face while looking legitimate, prior to putting on a better mask nearer the target.

Hair

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

Fingerprints

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

Maps

Essential but with pitfalls. A map found on you or near the event with markings and your fingerprints on it 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.

- If in doubt, buy new ones and use gloves.

Don't print off a map of the site you are visiting from your home computer, instead use an Internet café to do this. Another option is to buy a larger map of the region that contains the area you need.

Other materials

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

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 headlamps with red light for outside work—the light does not carry near as far as white light.

The vehicle

You want to keep it as clean as possible, especially if it is a rental 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 trash bags for disposing of the newspapers, etc.
- Have materials to wash mud of the side of the vehicle (mud can be used to pinpoint where you've been).

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

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

Disposing of equipment/clothes

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

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

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

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

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

If you are keeping equipment, you can wash it down thoroughly using soapy water or white spirits to remove trace evidence such as mud (though this will not remove, for example, DNA).

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

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

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

People have been caught because they simply tossed spray paint cans, bottles, etc. into nearby trashes and gardens, whereas if they had taken the time to put some distance they could have been disposed of innocuously enough.

Communiqués

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

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

Mobile phones

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 call a number outside of this small network, it is compromised. They should not be turned home near your homes. They should not be used until the day of the action (other than to charge batteries) at which point they are taken somewhere private (far away from your homes) and prepared.

Once the need for a phone is over take its battery out, and appropriately dispose of it and of its SIM card.

If the action only requires short-distance communication, consider using walkie-talkies instead of phones.

CCTV

CCTV is everywhere these days, but not impossible to hide from. Learn to recognize the various types of CCTV there are, but also be aware that they can be in stores filming what passes by the windows.[6] Quality does vary considerably on cameras, and some are decoys, so often they are there to act as a deterrent more than anything else.

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

CCTV also allows investigators to pick up on body language so no distinctive postures—keep to an ordinary straight backed walk.

A good site for dealing with CCTV is the Guide to Closed Circuit Television (CCTV) Destruction.[7]

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

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

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

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

---

[6] *N.T.P. note:* For an overview of the different types of CCTV, see You Can't Catch What You Can't See: Against Video Surveillance.[a]

[a] https://notrace.how/resources/#catch-see

[7] https://notrace.how/resources/#cctv-guide

Traveling

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

The best times to travel at night are around bar closing hours and after 4 a.m. This way you fit in with the flow of traffic. Some activists avoid traveling between 11.30 p.m. and 4 a.m., depending on the nature of the action—suggesting instead to park in a wood or similar and sleep until it's time to travel again. Beware of smoking if it is not an appropriate place.

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

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

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

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

Tip: Do not bring your mobile phone along as it can be used to track you.

A new development is automated license plate readers. This technology allows police to monitor passing vehicles with a camera and process the license plates with a computer. These readers are mounted in police vehicles, and increasingly integrated in surveillance cameras.

This will only work on legitimate license plates, and will not have any effect on bikes. It can also be partially avoided by traveling on country roads where there are less such cameras.

Being chased

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

On foot

Scatter in groups of between two and three, preferably matched by speed. Solidarity is all very nice, but there is no point everyone getting caught. Being matched by speed means you are not too spread out making you easier to spot—tight groups are better when moving through the countryside at night, as they stop people from 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. When doing preparation for an action run through routes to the rendezvous point (at least one person should have actually made it and know of any issues not identifiable on maps or of other dangers).

Always have a secondary rendezvous point and time if necessary. In this case people should have maps of the area (without markings) and/or be familiar with where they are and what they are looking for. There should also be a time limit on how long any pick-up vehicle will wait to pick-

up; again this is about not jeopardizing others who have already arrived by hanging around until you attract attention.

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

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

In the car

If you are certain that it is the police and not others who are onto you, you have nothing to lose—chances are that the driver will get caught anyway, but passengers still have a chance. Try and locate somewhere you can jump out of the car and run. If you are getting chased by workers or others who are likely to inflict violence on you, then you need to attempt to evade them.

We will not go into more detail on that here, but a search for "escape and evasion driving/techniques" or "emergency high speed driving techniques" on the Internet should provide suitable techniques.

Abandoning the car

If the car has to be abandoned, so be it. The people to whom it is registered to or who have rented it will still have to deal with the investigation so if they are not present they need to informed that this has happened, but watch out for late night phone calls that make them suspects. Remember to use a clean mobile phone and not one of the action phones. There may also be DNA left in the car that will implicate the driver and passengers, but this will take time to be followed up. This situation can lead to increased

monitoring of suspects for a while in the hope of finding more direct evidence. Be prepared for this but avoid raising more suspicion.

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

Some activists have effectively used false license plates to throw investigators attempting to trace the car. They often try to make sure the false license plate is from a car of a similar make and color as the one used in the action, so automated license plate readers don't trigger any alerts (e.g. wrong type of car or non-existing license plate). Vehicles also have chassis numbers and other serial numbers which can be used to trace the identity and history of the car should it be found abandoned, even if it has been burned out—though they are unlikely to go to this amount of trouble unless they are pretty determined to get the activists, and even then it may not actually lead to a chain of evidence. Burning the car will, however, likely get rid of most DNA evidence.

Evidence gathering tools

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

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

Debriefing

A useful thing to do for a variety of reasons. Security in debriefs should be as tight as when planning the action.

Some tips:

- 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 mistakes, but avoid attacking each other or putting blame on people for what was bad luck as that destroys group morale. A good debrief will help people grow as activists and/or show where people can be better deployed in future actions.
- Along with what went wrong, consider whether people are now at risk and what can be done. It should not be reasonable or useful to expect everyone to take the fall in solidarity with one person unless there exists a prior agreement to do this. However, it is important to arrange support for those potentially taking a fall so they are not left feeling isolated which could leave them vulnerable to breaking or dropping out of the movement.
- 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 thus making it less likely for them to talk to others. If someone feels the need to talk further they should not do it with anyone not involved in the action, but should instead 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 decisions. However, some degree of freedom for different group members to do the jobs allocated to them should be in place. With luck this part of the process should be a matter of simply checking off jobs done.

Shitting in your backyard

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

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

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

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

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

At some point you are going to make value judgments and go ahead with the risks. People have gotten away with surprising amounts of stuff relatively close to them by taking the right precautions; however, as a rule of thumb, interpret this expression as: **The more serious the consequences of an action the further away from your home you should be doing it.**

Conclusion

There is a lot of material in this document, 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 organizing a straightforward demo, you do not have that much to fear and a lot is inconsequential; consider about making life as difficult as possible for anyone investigating, but not to the point where the demo becomes impractical.

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

Security at home

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

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

If someone wants to discuss a sensitive issue take a walk, preferably in a direction you don't normally take. If you use the same route regularly for sensitive discussions consider changing it. Leave mobile phones in the house.

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—do not keep sensitive materials at home. Planning a process to deal with the risky information in your house will make this much easier.

Remember, if you are being watched any panicky action will be noted, thus bringing further attention on 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 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 project, as the phone calls made after a visit will receive more scrutiny and may signal other people as being worthy of attention.

Sensitive materials should be removed from your house on a regular basis in a calm manner—not furtively! This does not prevent you from practicing surveillance detection or anti-surveillance techniques, but do so discretely.

Any sensitive materials (including anything relating to a target, even if it is simply leaflets on related issues) should be dealt with before an action, not after. This goes for simple stuff as well—a magazine from Greenpeace can and will be produced as evidence to show that you are interested in anti-GMO issues and inferences can be drawn from it, especially if your target happens to be mentioned in it.

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

Depending on your location, you may actually be able to run away—as in one case where one activist in a house about to be raided grabbed the computer and fled into neighboring gardens, getting out of the area safely.

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

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

Being aware of intruders

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

There are few locks, if any, available to the average activist, that cannot be bypassed. However, if your lock suddenly gets stiff or develops a dodgy mechanism it could be the sign of a ham-fisted lock-picking attempt. Check for new scratch marks around the edge of the lock but ensure that they are genuinely new and not marks that you hadn't noticed before. It could also be a simple failure of the lock, so look for other evidence to back up your hypothesis before drawing any conclusions.

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

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

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

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

Tip: Possible hiding places for sensitive stuff are in bags or jars of food, though this will not fool everyone.

Being bugged

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

Bugs come in a variety of different forms and sizes and can be highly sophisticated. Most are now voice-activated and designed to blend in well. Old tricks such as running water and having loud music on in the background will not necessarily be effective against them. As well as breaking in, other ways of getting bugs into your house is through "guests," new appliances that have been intercepted, and gifts. Recently it has been reported that the police in the United Kingdom used wires to drop bugs into a house through eaves, thus avoiding them having to actually enter the house.

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

Nowadays, many bugs transmit their data through the mobile phone network such that the police does not need to physically retrieve a bug to obtain its data.

A search checklist:

- Open wiring points and check for devices being connected.
- Lift up carpets or probe their surfaces for bumps and wires. A common place is the edge of carpets at walls as they are out of sight and easy to put in.
- Air / ventilation ducts.
- Ceiling panels.
- Window frame moldings.

- Look for pinholes made in walls, etc.
- Top parts of doors, their frames and even inside door knobs.
- Behind pictures.
- Drawers, including their frames and undersides.
- Under tables, chairs & shelves.
- Devices connected to electrical lines outside of the house.
- Use ultraviolet (UV) light to detect if there are any changes in the paint.
- Check the back of furniture, including places where it might have been cut.
- Stereos, TVs and other appliances.
- Mattresses and pillows.
- Curtains, especially those with lining.
- Vases, plant pots, books.

Scanners

Scanners are simple devices that pick up on radio frequency transmissions; they can be bought in shops or over the Internet and are not usually illegal to possess. Follow the instructions on using them correctly. Normal practice is to go over the house with the scanner about fifteen centimeters from the wall, while talking constantly. Many bugs are voice-activated so as to conserve power so talking increases the chance that they transmit while you are scanning.

A major problem with scanners in that they are always one step behind the bugs themselves. For example, when cheap scanners started being able to detect transmission frequencies of 2GHz, bug manufacturers simply upped the transmission frequency to 3GHz. The real high-tech scanners cost in the tens of thousands of dollars and require professionals to operate. However, police and other investigators 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 scanners. On the other hand it can lead to a false sense of security, and removing bugs can encourage the surveillance operators to use more

effective techniques. If you find bugs your other security processes should protect you sufficiently anyway.

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

Your car, the garden & the environs

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

In a car, good places to look are:

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

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

High-tech surveillance equipment

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

Mention is often made of lasers being bounced of windows to listen to conversations. 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. Also, if you are taking the right security precautions, you will not be saying anything in your house which would compromise you anyway.

Your area and neighbors

It is good to know your neighbors, in terms of who 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.

Neighbors have been known to successfully rally around activists who have got into trouble. Neighbors (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 neighbors, in particular the "curtain-twitchers," and pump them for information on activists and their activities. Some go further and will provide the police with detailed monitoring of activists or even allow the police to place cameras in their own houses. The police may tell the neighbors outrageous lies about you in order to convince them to cooperate.

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

In one case an activist found out that there was a camera in the flat opposite them because the landlord of the block of flats was unable to keep it a secret and it found its way into friendly ears.

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

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

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

One final tip for your neighborhood is to get to know your housing project quite well. Watch out for cars being parked up in unusual places, or at junctions at the end of your road where they can watch which direction you are coming out of your house. Often these cars will be nondescript, but other than the person sitting in them for prolonged lengths of time, things to watch out for are lack of dealer tags, new tires and extra aerials on the roof. Even if people are sitting in cars with their backs to you, they can still be using the rear view mirror to watch. Work vehicles are also useful for surveillance—keep a close eye on what they are up to and which houses they are entering.

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

- Are the tires too good for the model?
- Is there a collection of maps in it?
- Have the details of the garage it was purchased from been taken off from the back windscreen or license plate?
- Are there extra aerials on the roof?
- Does the vehicle or its occupants turn up in other places you frequent?

- If the vehicle says it is part of a company, ring the company to check that it is genuine (you can use a storyline such as it is blocking your drive and you want to contact the driver).

Again any of these in itself is not evidence, but they all play into the pattern you are watching out for. Sometimes you will get a clear indication that a vehicle is State-owned such as a "police" marking on its tax disc.

Physical surveillance

Glossary

The following glossary lists terms used in the rest of this section.

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

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

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

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

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

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

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

Anti-surveillance: Taking action to lose a surveillance team.

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

Active detection: Taking measures to identify surveillance by taking evasive measures. Can be overt or covert depending on whether you want to avoid alerting the surveillance team.

Target pattern analysis: A study of the target identifying their habits and other routines, allowing for easier surveillance.

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

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

Introduction

Being put under physical surveillance is a fact of life for the political activist. It is actually a sign that you are being taken seriously so it is not always something to be concerned about. It is certainly not being paranoid to think that it could happen. It does, and much more regularly than is supposed, though not often in a systematic manner. There is no basic right that stops you from being put under surveillance, so relying on the law or the fact "you are not doing anything wrong" are no protections.

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

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

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

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

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

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

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

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

The main question the activist needs to ask themselves is how they want to deal with surveillance. This may have significant consequences both for the reaction of the surveillance team and the activist's actions. If you are not particularly engaged at the moment in activities you would rather the State did not know about, or they are simply doing routine surveillance

to update their files, then we suggest, as a rule of thumb, that you do not let them know that you are aware. Instead, avoid drawing further attention on yourself and focus on confirming whether you are actually under surveillance or not. Save active anti-surveillance activities for those moments when you need to confirm that you are indeed not being followed before potentially compromising yourself or an action.

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

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

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

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

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

future, and it brings attention to yourself so encourages the use of more sophisticate methods.

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

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

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

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

the more discrete you are able to make it, and the more you develop that important instinct.

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

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

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

Preparation for detecting surveillance

The core of surveillance is target pattern analysis. That is, the study of the routine and habits of the target, the person being followed. This covers many things, but in particular stuff such as: what are the regular routes they take to and from places, their driving style, who they visit and so

on. What the surveillance team seeks to do is to be able to predict your movements to make themselves less noticeable and the surveillance job as a whole easier and less resource consuming. Do not assume that because stuff feels obvious to you, such as how you get to and from work and where you work, that it is obvious to them. They still need to confirm it.

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

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

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

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

How you plan your surveillance detection depends greatly on what your intention is. You need to decide if you are going to let on or not; if you are planning to lose them or if you don't really care at this stage. Sometimes this will depend on the day. For example, if you are part of a large public event they may start attempting covert surveillance on you hoping that you

will lead them to anything planned they may not know about; however, if it becomes clear that you have burned them then they are likely to switch objectives to simply keeping tabs on you with the command operative that you have identified. This is to disrupt your activity, as they may assume that you are some sort of crucial organizer.

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

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

Surveillance team techniques

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

Trigger

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

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

Command

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

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

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

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

Observation points

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

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

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

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

Stakeout box

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

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

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

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

Lost command routine

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

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

Exposure

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

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

It is also worth allowing patterns to be established as this lulls them in to complacency and dropping their guard slightly—surveillance is hard to keep up for a prolonged time at the same level of intensity. Thus, when you break the pattern, they are more likely to show their surprise. When

you are traveling a route not normally taken, or that is new to you, then they are automatically more alert to your actions.

What to watch out for

Vehicles

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

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

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

On foot

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

- Coughing, tripping and other behaviors of someone who is being distracted when there is no obvious reason for it.
- Signs of tensions such as pacing, focused staring, checking the time repeatedly, twitching.
- Awkward mannerisms in general.
- Speaking into collars or their chin lowered into their chests as they speak.
- Touching their ears repeatedly is instinctive reaction to an ear-piece in use.
    - Is there a wire running down to their collar? Though with the prevalence of personal stereos and MP3 players this is far more common place and harder to detect unless it really looks out of place with the rest of the person's attire.
    - Do they stop and stare into nothing—a feature of someone taking a message.

- Adjusting clothes hiding communication devices or repeatedly putting their hands in their pockets to manipulate a communications or listening device.
- Clothes out of place for the venue (e.g. a suit in a punk venue, etc.)
- Startled look as they encounter you unexpectedly in active detection techniques.
- Bad window-shopping (compare how people usually do it by moving their heads, as opposed to a tail who is trying to see in the reflection or not properly looking at all).
- The same person taking yet another phone call.
- Avoiding making eye-contact at all cost.
- General uncertainty after you break an established pattern.
- Are they carrying a bag with a video camera in it?
- Carrying out repeated scratching of head or checking of watch—possible non-verbal communication signals.

Appearance

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

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

Night observation

At night the world is a different place; you need to be in tune with how noise and silhouettes change in the dark. Likewise it is worth developing your night vision: this takes about 30 minutes and you need to avoid bright

lights or you will ruin it. When looking at things use off-center viewing or scan rather than looking directly.

Remembering details

For vehicles, things to look out for are:

- Body shape.
- Shape of headlights.
- Dents or scratches or other distinguishing features such as broken lights.
- Silhouette at night.

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

- Facial hair.
- Hair color.
- Unusual features such as scars.
- The shape of the face.

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

Vehicles

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

Urban

Passive detection

- When going to and from your car use the opportunity to look at the surrounding area for people or vehicles that might be acting as triggers for the surveillance. Depending on the area the trigger may be on foot as opposed to in a vehicle. Try not to stop and stare but make it natural. If you've already worked out where in particular you should look it becomes quite easy.
- Are there vehicles near your home, work or places you frequent regularly that have people sitting in them? Often they will have their sun visors down permanently; this is done to stop faces being fully visible. This is surveillance that is poorly resourced or where they want you to know they are watching you.
- License plates:
    - Memorize license plates: if you spot a car you are suspicious of, look at the license plate and turn the last three letters into a word, e.g. BCH becomes BaCkHand. Words are easier to recall than numbers and letters, and if you come up with the same word again you can pick up on it quicker.
    - Watch for license plates that do not have a garage name on them; police tails are often missing these. Note, this is not a guarantee the vehicle is definitely a tail. Some unmarked police cars actually have police written on their tax discs.
- 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 security at home for more on what to look in a vehicle parked up like this.
- As you pass identified pick-up points, watch the parked vehicles. Often they will park in the same direction as you normally take and on the same side as the flow of the traffic.
    - Can you see maps and signs of people sitting in them for a while, e.g. coffee cups, food packets on the seats?

- If possible check the exhaust to see if it is running and waiting to go.
- In cold weather are they getting out to clean the windows regularly?
- Do they pull out behind you as you pass?

- Vehicles tailing will generally drive two to four cars back. Depending on the nature of the traffic and the road, they need to keep you in sight, so watch out for vehicles pulling out of the line of traffic (both sides) and then drifting back in. There will be points at which they close up on you, depending on obstacles and other traffic situations, e.g., road works, traffic lights, heavy traffic. This gives you a chance to get a closer look at them. One bit of suspicious behavior is when a vehicle slows down prematurely so as to avoid coming right up behind you, thus upsetting the flow of traffic.
- At junctions, traffic lights, etc, the surveillance vehicle will often get closer to the target vehicle to ensure they can see which direction it is intending to head in. However, if they feel that it has become too exposed it may turn in a different direction to be replaced by another vehicle, though this depends on the resources at hand. If you suspect a vehicle and it does turn off, still keep a note of its details in case it reappears at a later time or day.
- On longer stretches of roads, surveillance vehicles will have a tendency to pace each other in a convoy; that is match each others speed and keep the same distance apart; they are unlikely to overtake each other. This becomes a recognizable pattern that can be spotted. They will be in front and behind the target vehicle, with the ones in front allowing the target to overtake as command is changed around to avoid the target getting suspicious.
- They will also pace themselves to the target vehicle. This allows them to be spotted through careful observation. For instance, depending on how they change speed, they will travel fast to catch up with you. As they get close to you they will slow down and pull back instead of overtaking as you might expect. Do they drop back to the same distance they were previously?

- Adverse weather conditions will cause surveillance vehicles to drive closer than they normally would due to poorer visibility; in particularly bad weather they will drive in front of the target vehicle.
- 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 may briefly turn on their headlights so they can read your license plate, then either pull back or overtake (before falling back later). If you believe you are being tailed, keep an eye on cars that do this.
- Enter a gas station and see who else follows you in. Is there a car that is not refilling or simply parks up? Does anyone follow you to the shop but doesn't buy anything? You can also use car parks for this, but they are harder to use to confirm suspicions given their general geography, though it does allow you to narrow down the set of vehicles to be considered suspect. Likewise with a lay-by on a highway or main road.
- If you are in a service stop or gas station for some time then a stakeout box will be set up around it (or in it, in the case of a service stop). This provides opportunities for you to look for the tell-tale signs as you return to your car or leave the site. As you do so, take one of the nearby side routes as opposed to the main road, if there are such opportunities. This is were you are likely to encounter surveillance team vehicles waiting—they may be parked facing away from the gas station, etc. in case you did take this route, but they still have to pull out and follow you, thus giving themselves away to the person who is watching for it. If you are able to observe on the way into a gas station you may actually witness the surveillance team set up their stakeout box.
- Stopping to eat in service stops gives you an opportunity to monitor faces and vehicles coming in. If you are placed at a window you may spot them checking your car for writings/maps/papers with directions as to where you are heading.
- In a multi-story car park who follows you all the way up to the top floor to park?

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

Active detection

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

- Erratic driving includes:
  - Running red traffic lights, or attempt to clear them just as they are turning red; often surveillance teams will not follow as it exposes them so this is also an anti-surveillance technique.
  - Cutting down side streets (beware of picking up surveillance vehicles moving parallel) and other shortcuts.
  - Illegal turns.
- When you take turns or side streets there is a possibility that you will encounter one of the other vehicles in the surveillance team, perhaps one that has previously been command and you have already been suspicious of. Thus you should look to see what other traffic is also appearing as opposed to what is behind you.
- Pull into the side of the road at a green light; who else waits behind rather than go through?
- If you are aware of a blind turn or a sharp hill, drive fast into it and once through it slow down immediately. What vehicles are bearing down on you as they attempt to get you back within sight? Do they decrease speed rapidly to stay behind you or do they realize they have been burned and overtake to get out of the area. A variation is

to pull in immediately and look for the reaction of suspect vehicles passing you.

- Do a U-turn.
  - Look out for:
    - Who attempts to follow?
    - What vehicles behind you attempt to park up? Do they turn in your direction in an attempt to pick you up again?
    - What is their reaction as they pass you?
    - A variation is to pull in and wait for any suspect vehicles to pass you before doing the U turn.
  - In light traffic these reactions will be quite obvious, and in heavy traffic they will cause commotion, both effects playing into your hands.
  - Standard practice for the professional is to continue traveling on and not turn until the first opportunity comes along rather than doing their own U-turn. However, in our experience this is a good method for exposing the surveillance tails where there are fewer resources available to them.
- 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.
- Take roundabouts several times (though under United Kingdom law three is the maximum number of times that you are allowed to this), though the successfulness of this depends on the size of the roundabout, the heaviness of the traffic and how far back the tail is.
- Signal as if to turn at a junction and then go straight on. Has the suspected tail done likewise? This not particularly effective as tails may not signal at all because of this and being several cars behind means that they can react to your change without giving themselves away. Works best for where the car you suspect is immediately behind you.
- When parking on a street choose a direction opposite to the one you leave in. Allow enough time for a stakeout box to set up. You are looking for uncertainty in the trigger on the unexpected behavior, or vehicles doing inappropriate U- turns to stay in the same direction

as you. It also means that more resources have to be committed to tailing you thus increasing the chance of detection.

- Cul-de-sacs are ideal for picking up on tails, and with amateur tails for losing them. However, your tails are also aware of this. Go down the cul-de-sac and wait a few minutes before leaving again.
    - The tail will do one of two things:
        - Follow you down the cul-de-sac (though you may need to allow them a few minutes to make this decision). In which case you can immediately spot them, especially if it is a car that has been with you for a while. Plan to turn your vehicle as soon as possible though out of site of the road you've come from. On a narrow cul-de-sac you can be gone before they have a chance to turn around.
        - Wait on the road outside the cul-de-sac knowing that you are practicing anti-surveillance techniques. As you stop at the top of the cul-de-sac waiting to rejoin the flow of traffic, watch out for cars parked up with the entrance of the cul-de-sac in sight and that start moving once you leave the cul-de-sac. Driveways may be used as well, but may require high enough housing density to work.
    - If the cul-de-sac is signposted and your tail is professional then they will not be caught out by this, but it still often works on the average investigator or police who don't have much experience tailing people who watch out for surveillance.
- 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 the tail will actually stop. Further up or around the exit point is usual. As by this time it is probable that they realize they've been burned. However, unless it is a heavy-duty operation, they will quite often wait around to see what you will do anyway. In this case we suggest that if they have already been in a position to see the faces of who else was your the car, then you pull along side them to have

a good look at their faces, even photograph them (you have a good excuse by saying that you thought they were trouble, though it in turn could be inviting them to harass you further, so balance out the risks), even ask them a question for directions. It allows you to find out what they look like, while at the same time letting them know their cover has been blown.

- Use routes that are not obvious to get to your destination such as taking the long way around an estate or several blocks when there is a blatantly easier way to reach it. Works better for a destination they are not aware you might be heading to. It can be a destination you have picked solely for this purpose.
- Having left your starting point, take a different route back to it. Does anyone follow you back, even to the end of the street?
- Highways and other major roads provide different opportunities for spotting the tail. As the travel on them is faster the command vehicle and their team also need to be able to react faster to keep you in sight. They may have to allow for the fact that if you come off at a junction they need to see which way you have gone. However, at night and on roads with long-range visibility and low density traffic it may be that they do not need to be as close. Remember though, that if you force the hand of one surveillance vehicle, then it may be replaced by one traveling further behind it.
- Who follows you into a service stop or over a junction and back onto the motorway? This is not typical behavior, but if they want to keep you in sight they may have to commit to it, though if a professional realizes what you are doing in time they will lose you but let a vehicle further back pick you up further down the road. However, you have potentially taken one vehicle out of the operation. This is not a tactic that will work with repetitive attempts as they will soon get wise to it. A more covert method, if you are not ready to let on you've identified the vehicle is at a complex junction to go around in an odd way that takes you back onto your original route, or even in the opposite direction. Which vehicles have had to get close to follow you and also taken this odd path? This may require some prior planning to be successful against an experienced team.

- Slow down to exit onto a service road or junction, but at the last moment pull back out on to the main road—who does likewise?
- Just before an exit from a highway pull into the hard shoulder. Standard procedure is that the command vehicle will leave at that exit so you may be able to identify them.
- At tolls choose the longest queue to go to. Who does likewise? Does anyone go through and pull up or drives slowly until you pass by?
- If you are pretty confident that the vehicle right behind you is keeping you under surveillance, do an emergency stop that forces them to go into the back of you, or come very close. Get out and check their reactions—often they will simply drive off rather than engage with you. If you are a bunch of big men getting out aggressively they may drive off out of pure fear rather than because they are tailing you. If they don't it gives you a chance to confront them.

Anti-surveillance

- The best way to lose a vehicle from home is to follow an established pattern to start with, then to suddenly break it by taken unexpected turns or traveling at speed down roads, thus forcing them to take a choice of either losing you to avoid exposure, or exposing themselves, so effectively taking themselves out of the surveillance team.
- Both situations are opportunities to be taken to lose them, and move out of sight altogether. Techniques for doing this are extensions of the various active detection methods above, where instead of watching for reactions of possible tails you are using the opportunity to get away from them altogether.
- If you are aware of a blind turn or a sharp hill top which cannot be seen over, either of which has a second turn immediately afterwards, you can use this to get out of sight.
- If you are using vehicles, park up where you have quick access to a foot only route taking you to another road where a colleague is waiting in another vehicle to whisk you out of the area.
- If you know an area well, then consider concealment in little lanes and long driveways, though this is very much dependant on the terrain

and how well you can remain concealed while they are searching for you.

- Go for dense traffic, and weave in and out of it. It is much harder to follow someone in these circumstances; use routes they are not likely to have anticipated.
- At night switch off lights and pull into concealed places or even driveways (use unoccupied houses or pretend to be lost to the owners).
- Bikes are much harder to follow than vehicles; especially in places were there are many cycle paths distinct from roads, allowing you to disappear out of sight. It is easier to lose foot surveillance, and easier to detect if anyone is attempting to follow you, as other bikes tailing you and especially cars stand out a lot more. Planning is still needed as other members of the surveillance team may be waiting at the end of the cycle path for you to reappear.
- How to deal with static observation vehicles, or even individuals?
    - There are several options:
        - Call the police on them with a story of why you suspect the vehicle and observe the reactions of the suspected surveillance. Often the police will not turn up, but the surveillance vehicle, knowing they are now being watched themselves, will move shortly afterwards.
        - If you have a back way out of where you are that is not regularly used and thus unlikely to be watched as closely, sneak out and around to get close to the observation vehicle. At night this can be used for covert surveillance of the vehicle to see if there is anything further to add to your suspicions. The chances are that you will be detected doing this, but it will be enough for the team to assume their cover has been blown.
        - Monitor the driver of the vehicle to see if they are being picked up nearby after leaving it, or have a secondary vehicle stationed nearby.
        - Openly take photographs of the vehicle to scare it off.

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

Rural

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

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

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

In rural lanes you have several options:

- Get out and walk up to a house or into woods, thus forcing the command to give themselves away by following or abandoning you. Longer paths which allow you to get out of sight and double back are useful for seeing if anyone has pulled up and is waiting.
- Drive into a farm and turn around, giving suspect tails enough time to pass, then drive off in the opposite direction. If you know the area

quite well, it means you can take a route that is hard for them to pick you up again.

- Use the narrow roads to your favor—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 GPS bug (possibly also capturing audio) is attached to the underside of your car allowing it to be followed at a distance. This is one reason why using your car to go directly to secure meetings or high-risk covert actions is not a good idea, as the chances are you will not locate the device.

This being said, there are ways of testing to see if you have one, though not necessarily foolproof:

- Use a radio frequencies scanner to detect transmissions from the car.
- Drive into the countryside, park up and wait in an adjoining field to see if anyone comes along to check out why the vehicle has stopped. Tails picking you up when they really should not have is another sign they may be using a bug in this way.
- Stand next to the car with a friend and discuss a fake action to see if it provokes a reaction later on.

On foot

Urban

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

Passive detection

- Enter a shop and watch who follows you or who waits to pick up on you again as you go out. Watch for people staring into shop windows. Often their body language will give themselves away as they are not doing it properly. It is useful to practice watching people in the street on how they window shop and such like before doing this so you can pick up the nuances that distinguish between someone doing it genuinely and those whose attention is elsewhere (like trying to spot you). Check where their eyes are looking and whether they are doing more than simply staring ahead.
- If the shop has a back entrance leave through it, and promptly stop around the corner to see if anyone else is looking rather hurried as they try to catch up with you. Look uncertain about the direction you are taking or look at your watch if you want to avoid being obvious that you are waiting to spot them.
- Stop at a cinema or theater and read the boards there. This gives you an excuse to stop and look around.
- If you go into a shop or an alleyway you do not normally go into, is there anyone who crosses from the other side of the road you were on? Depending on what you have entered, what do they do? Do they follow or do they hang out opposite the entrance? If it is a small shop then they are not likely to come in as it would get them too close to you (unless they are interested in your shopping habits). If the shop or café has largish windows then you can use them to watch activity outside to see if anyone is loitering around.
- Professional tails will be ready for you to duck into a shop or to do "window shopping," so they will simply pass you by. Thus while you are looking for people also keep watch on those who have passed you by and then stopped.
- In a café or similar choose the seat which allows you to view as many people as possible, and definitely face the door.
    - Keep an eye out for couples who are not chatting or not acting naturally. It has happened that while a group was relaxing in a bar surveillance team members have come in and sat next to them with bags containing listening devices. They gave themselves by

their body language, consuming their beer or food slowly or not at all, and had very poor interaction among themselves, instead watching people from the group going to the bar or toilet, etc.

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

- In a bookshop is there anyone looking at the same books that you just browsed through, especially 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 does likewise?
- Stairs and escalators in a shop give opportunities to look for tails. Approach them from the opposite direction so when you reach them you have to do a half circle turn, and are thus able to look behind you without appearing to do it deliberately.
- As you leave a shop, stop and ask someone the time or for directions, keep an eye on who might have followed you out, or is waiting nearby.
- Choose a narrow or quiet street to act as a choke point to filter suspects out from the crowd making them easier to identify. Doesn't always work with a professional team as they will be prepared for this. If this is not a place you would go in the normal course of business then it becomes active detection.
- If in a train or bus station, change position regularly and watch those standing still. Keep an eye out for people not reading timetables or properly paying attention to their phones. 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 approaching a place you plan to use as your own observation point, check out who is already there to eliminate them from consideration.
- In areas that are not a city center or are low on pedestrians in general do vehicles at stakeout points pull out and travel slowly behind you? More professional ones will move ahead of you and wait for you to pass.

- Enter a place where an unprepared tail will look out of place, e.g. a punk shop, etc. If this is not an obvious place for you to be in then this becomes an active detection technique and thus 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?
- Given the increasing prevalence of CCTV cameras in cities, and not just in the centers, watch out for those which seem to rotate in your direction. With this, it is good to know where they are in advance and be discrete in your monitoring of them. If they do not think you are being aware of possible surveillance then they are unlikely to be discrete themselves.
- Is there someone hanging around your street with a camera? This has been known to happen with amateur surveillance teams.
- Shopping centers are awash with opportunities to put the surveillance team on their toes, as there are many observation points available as well as exits. Balconies are ideal for watching those coming in behind you, as are see-through elevators. If you can get into an elevator fast enough you may have a get-away route through passageways to nearby buildings or car parks. Other tactics worth mentioning is to use little used exits to draw out who is following you; or enter shops at the last minute when it looks like you are about to leave. Standard procedure for surveillance teams is to cover all exits.

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

Active detection

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

- An empty street is a good place to spot or lose a tail. Try doubling back, watching for people walking past slowly and watching, etc.
- The main tool for detecting foot surveillance is the blind corner, which works very well with amateur or incompetent tails. By taking one you are setting up an opportunity to check reactions, by doubling back on yourself which they cannot see so are not prepared for, or by simply stopping and watching. If there is a café or shop with a good window just around the corner then entering that allows you to give them the slip or to observe their reactions. However, a professional tail will actually walk on rather than go round the blind corner, and use their communications gear to get another member of the team pick you up.
- When you go around a blind corner, consider ducking into an office block and concealing yourself there; this is worth doing if you are quick thinking and able to bluff receptionists.
- Double back on yourself, and repeat to see who you keep spotting. Tails will avoid making eye contact however, and will attempt to dress for the area they are in so it may not always be able to spot them. What you are looking for is the uncertainty that you have just caused them as they decide how to react to your change. A professional will be on the other side of the road rather than right behind you. Rather than just turning around, cross the road and then go back in the direction you came. This is active detection, but it is much better at forcing them to react and you have a good opportunity to gauge reactions. This is much more effective on narrow terrains such as foot bridges where there is not much of a gap between both sides and little traffic so you can get to the other side relatively quickly.
- Waiting in a queue for a bus is a useful method to spot tails and lose them at the same time.
    - To spot the tail let a few buses go by to see who else is waiting (at the bus stop or nearby)—particularly useful if someone gets on a bus with you when one going in the same direction has already passed by.
    - To lose them, you can suddenly "realize" that a bus across the road is the one you want and make a dash for it; it is a good way

of losing a tail and potentially exposing them. Alternatively, drop out of the queue as you are about to board.

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

Anti-Surveillance

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

- Don't wear clothes, jewellry or hairstyle that stand out as these simply act as marker for them and means that they can be more discrete in tailing you. Surveillance teams focus a lot on clothing, so make it nondescript and common.
- You can also bring changes of clothing and appearance (e.g. wigs) with you. Wigs are particularly effective, but only if they are cut to look good; badly fitting wigs only draw attention. As well as change of clothes have a second rucksack or bag to carry them in—avoid using the same one with different clothes.
- Some quick ways to loose a tail are:
  - 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.
  - Have a friend pull in and pick you up from a route where the surveillance team will not be following you in a vehicle. It may be that this can be done discretely with you hiding in the back under a blanket, but tends to work only where they are not expecting it and they are not familiar with the vehicle or the driver.
  - Get lost in a crowd—a classic, but it does work. Factories and football matches are good for this as well as city centers, which

is why it is worth knowing the area if this sort of event is a possibility.

- Shops with multiple and/or out-of-the-way exits are good for both active surveillance detection (wait next to an 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 never go into, or if you do, you always use the same entrance and exit.
- Elevators that take you to other floors with exits are good; remember though that the surveillance team will leave someone at the ground floor in case you return there.
- Places where there are security checks can work in your favour, especially where there are multiple exits, as surveillance teams will be reluctant to set off alarms with their communications gear. The delays for stop and search also play into your hands.

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

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

Remember, one or two coincidences are not proof you have a tail. You are looking for a whole series of them. Practicing surveillance detection and anti-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 guess your destination and route, and monitor both as well as having someone on the same bus or train. This means that depending on numbers they will seek to reach possible exit points to watch for you. If it is a public transport route that you use frequently, they will either follow the bus (something you can watch out for) or be waiting to pick you up at your destination.

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

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

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

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

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

Regarding trains:

- Given the nature of trains you are more likely to have a number of surveillance operatives get on and off the train at the same time as you.
- The more you change trains the more it erodes the integrity of the surveillance team. Add to this by going to the barriers as if leaving then turning around and getting back on another train.
- There are a number of exits for stations which you can use to your advantage, depending on crowd density and how well you can push through them.
- A good feature of train stations (though it works well in other areas with a high density of pedestrians) is that there are strong flows of

people in one direction. If you move against this flow, watch out for others doing likewise and struggling to keep you in sight. As you have to look as you do this, it is an active detection technique.

Night surveillance while on foot

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

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

- Driving without lights.
- Lights going on and off in stationary cars.
- The sound of radio transmissions.
- Doors slamming shut as you approach.
- Vehicles parked in unusual locations.
- 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 this situation. If you know your area well then you can spot them by being parked in places not normally used by them. For instance, police cars do not normally hang out in wealthy areas. Taxis do not wait on poor and out of-the-way areas. People waiting on friends at nearby houses tend to park in the light and on the main road and not in out-of-the way places offering concealment.

Some tactics that work better at night are as follows:

- If you think that someone is following you, listen out carefully for the sound of their pace. It will be done to match yours, such that as

you speed up and slow down, it changes 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 if they are innocent they will pretty much react in the same startled way, thinking you are a mugger. However, you can get up close and ask for directions, a cigarette light, etc. which will put the suspect tail on the spot and give you a good chance to look at them, something they will really not like.
- Taking blind turns at night forces the surveillance team to react more aggressively, so again forcing their hand if you are ready for it. However, given the darkness there is a possibility they will react more confidently if they think they have the upper hand.

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

Rural

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

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

Things to check for are:

- Repeated glints off binoculars from woods or copses.
- Abandoned buildings they are using to hide vehicles.

- 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, copses, thick bushes/hedges that have a view of the target area.

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

Counter-surveillance

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

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

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

- The surveillance team may be aware of who your friends are so will be able to recognize their faces; if engaging in this sort of operation, consider some sort of change of your normal appearance or disguise.
- The security around the setup 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 and expect it.
- The counter-surveillance team needs to be able to move swiftly and discretely; this may include hand signals that are not too quick so

others can pick them up (e.g., outstretched hands as opposed to a quick scratch of the chin).

However, it is important that this should not be 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.

Blatant surveillance

Much of what has been said also applies to being chased, that is, 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 lose them. Be unpredictable, use public transport and sometimes just run (that is not illegal in the United Kingdom so it is not grounds to stop you, though that may not bother them). It depends on the situation, whether you publicly burn them to people around you, or discretely lose them.

The other approach is to be completely innocuous and ignore the surveillance: have a coffee or a beer or simply shop around.

Talking to others about security

It is important to discuss security in your group. You need to make sure that your affinity group or organization can be trusted to look after itself, and that weaknesses are minimized according to the threat you are likely to face. However, there are several pitfalls here you need to watch out for.

- If you go over the top, then you risk putting people off, scaring them or otherwise disempowering them. Encourage people in your group, especially those less experienced than yourself, to think about their security needs, and how lapses in security can affect other people but don't enforce without explanation. Be wary of letting a "more-secure-than-thou" competitive attitude develop as in a group as that is very off-putting; likewise with installing a paranoid mindset rather than an active one. As you develop the security mindset, it is easy to lose understanding about how people who are new to the scene think. Do not oppress them for getting things wrong, but do suggest where they can make changes. Explain to them why you carry out certain processes, and encourage them to ask questions—otherwise they'll never learn and you could be jeopardising yourself. Don't panic if new people start asking about security and other issues; it's how people learn and develop. If you are not going to provide an answer, explain why without being condescending.
- If you see a security lapse in someone else, there are several ways of dealing with it:
    - Bring it up as a general point at a meeting in a sensitive manner without particularly naming and shaming. This has the advantage of reminding others of their responsibilities as well. Shouting and ranting is not beneficial to anyone.
    - Take the person aside and explain your concerns, explaining that you feel uncomfortable and why. In particular, say that it is you who feels at risk. If they do not sympathize with you they are less likely to pay heed to your request that they improve their security so let them know that you will have problems with working with

them in the future. You can also ask others whom they may have higher respect for to also approach them.

- Don't boast about your own security precautions. Security by obscurity is not a sensible approach; however, using obscure ideas to improve on your security is a useful technique, but only works as long as it remains obscure. Beware of your own ego on this one. You can suggest techniques in general, but the actual bit of cleverness, keep that to yourself. For example, if you use Finnish words for your password, you can maybe say that you use a foreign language; just don't say which one.
- Don't give bad advice, or make things up rather than appear ignorant. Security can change quite rapidly, especially with scary developments like RFID chips, improved biometric techniques, etc., so if you don't know the answer then it is better to say so than to lead someone into a false sense of security.
- Watch out for people who are not acting as securely as they claim to be; the question then is if they are prepared to lie over one bit of security, then what else are they maybe lying about. Give them a chance to change, but if they don't, then take precautions to ensure that they do not end up compromising you.

All this aside, just because someone is not at your level of security does not mean you should never trust them. They may not know all the ins and outs yet. An action, especially a low-level one, can be an ideal time to teach by example up and coming activists what they need to be doing, while at the same time actually doing something to justify it all.

Future developments

As technology develops, there will be advancements in methods of forensics, of biometric identification of people, and also in tracking devices. These are the three main worries activists have in terms of security. However, there are pros and cons here, and don't believe the hype.

Biometric recognition techniques—such as face recognition technology—are proving not to be as good as claimed. With face recognition, the problem is that there are two many false positives, that is, too many people are being picked out as possible suspects compared to the actual number of suspects there is. This somewhat contradictory situation means that not as much is gained from this technology as hoped as users of it have to spend as much time dealing with the false positives as following up on the genuine leads.[8]

Saying that, CCTV is improving widely in quality and also in distribution, and now beginning to include microphones.

The police do not have all the technology they make out to have. In the United Kingdom, technology comes through a non-public body called the PITO (Police Information Technology Organisation), which evaluates and buys in new technology for the police to use. So when it is trumpeted that the police have a new technology, what it really means is that the PITO have got it, and not necessarily individual police forces. They have budgets to adhere to, and thus try to buy the stuff they really need, meaning a lot of the fancy high-tech stuff is actually not used by the majority of forces.

The main changes of relevance to activists are:

- Improved forensics catching traces that would have previously been missed on materials, etc.
- Improved data exchange between police organizations and between the police and various other holders of personal information such as

[8] *N.T.P. note:* Unfortunately, as of 2025, facial recognition technologies are becoming quite good and are not turning up as many false positives as 20 years ago.

banks. This also includes improved processing and cross-referencing of information (see also the risk of compulsory ID cards).

- Increasing sophistication of listening and tracking devices, in particular in transmission range and in miniaturization.

However, there is hope—and it comes in the form of budgets. The promise of high-tech equipment and techniques is as much about saving costs as it is about effectiveness. As security agencies come to rely on them, they will rely less on low-tech and manpower intensive techniques (such as active surveillance).

The result is that low-tech security precautions can actually become more effective—bugs only work if they can be placed somewhere you are going to be talking; using ATM machines and credit cards to tag you cease to work if you pay only in cash. This is why we are confident that activists will continue to be a thorn in the side of the status quo despite constant repression from the State and corporations.

This re-edition contains a wealth of information to help anarchists and other rebels analyze their security needs, plan and carry out direct actions, and detect or evade physical surveillance. We hope it will help you defeat the State and achieve your goals. Good luck!

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.