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!

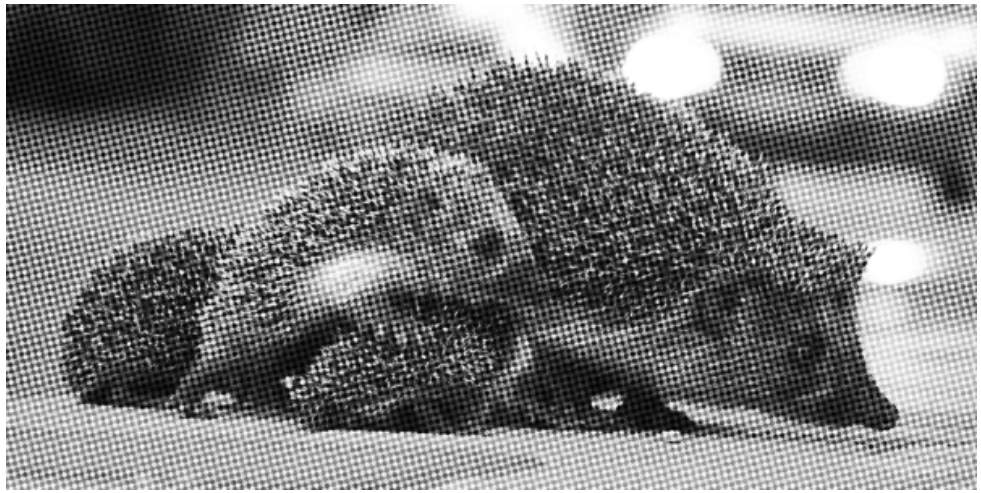
No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

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.

A Practical Security Handbook

No Trace Project edition

Part 1/2



A Practical Security Handbook: No Trace Project edition
Part 1/2

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

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.

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.

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

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.

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.

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 proactive 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.

- 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.

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:

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

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

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.

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 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

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 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.)

- 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

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.

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 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

[2] *No Trace Project (N.T.P.) note:* For more information on this episode of repression, see the 2008 zine Green Scared?.[3]

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

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

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

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.

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)

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.

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.

aware that they can be in stores filming what passes by the windows.[12] 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.[14]

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.

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

[12] *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.[13]

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

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

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

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

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

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

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.

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.

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.

- 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.[4]

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

[4] *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.[5]

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

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.

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.[6]

Clothing & other traceables

During the action itself, you will leave a number of traces behind that forensics can use to investigate.[8]

[6] *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.[7]

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

[8] *N.T.P. note:* For information on forensic traces, see our Threat Library's entries on DNA,[9] trace evidence[10] and fingerprints.[11]

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

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

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

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.

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