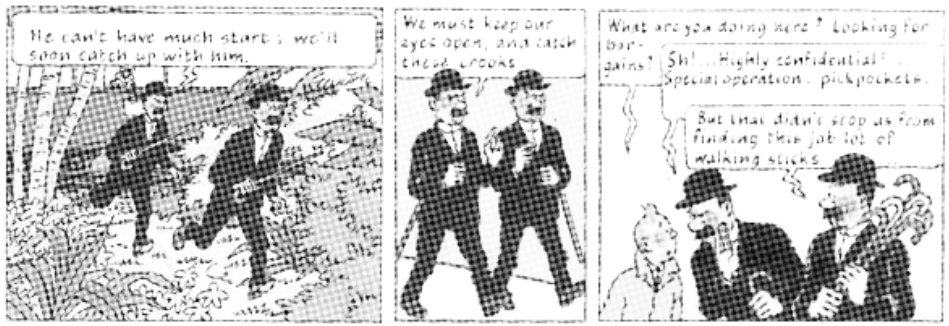
In our experience, we have found that it is often difficult to find an overview of different forms of action, especially militant ones, as well as practical and contextual thoughts on different aspects of security and action planning. […] That's why we have collected information about taking action.

PRISMA

Primer on Radical Information for Secure Militant Actions

Part 2/2



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.

PRISMA: Primer on Radical Information for Secure Militant Actions
Part 2/2

Original text in German

PRISMA: Prima Radikales Info Sammelsurium Militanter Aktionen

2010

web.archive.org/web/20250611231250/https://militanz.blackblogs.org/wp-content/uploads/sites/481/2017/11/Prisma.pdf

Translation and layout

No Trace Project

notrace.how/resources/#prisma

5. Documentation

[…][32]

Photos of Actions

Just a few little tips:

We strongly discourage you from taking photos of actions in which people can be seen! Even if they are masked, they may be identified later. Even if you pixelate, people can also be identified by their body shape and clothing, and not all methods of pixelation are effective. Some image distortions, for example, can be easily reversed by police technicians. Some photo software also store a copy of the image before pixelation in its metadata, though there are programs that remove this additional information. If you post digital photos online, remember that the image file may contain metadata about your camera. There are also programs that delete this information, but we don't know how effective they are. It is also possible for a camera to be seized before the photos it took are anonymized!

[32] *N.T.P. note:* The majority of this chapter has not been included in this translation because we deemed it outdated. For more information about digital security, see our Threat Library's "Digital best practices"[a] mitigation.

[a] https://notrace.how/threat-library/mitigations/digital-best-practices.html

- Clean up the places that could be searched: apartment, attic, basement, car, garage, etc.
- Think about places in your home where you cannot be observed, whether it's possible to leave the house unobserved, or how you can otherwise inconspicuously evade surveillance if doing so becomes necessary.
- Avoid any behavior that appears “conspiratorial.”
- Try to develop a daily routine for yourself in this threatening situation.
- Write down your observations and evaluate them with your friends.
- Develop a hypothesis about the reason for the surveillance that you can deal with. Think about perspectives for your future actions.

The worst-case scenario for the surveillance operators is that the target has turned the tables and is in control of the operators!

The worst-case scenario for you is being reckless and burying your head in the sand! But the second worst-case scenario is panic and paralysis!

To all those who are wanted or under surveillance, we wish you all the strength you need. Let's use knowledge against paranoia!

Contents

will stay calm and pass on the necessary information to the right people. You may be able to find out who the surveillance is targeting. If so, that should be the end of it for you. It might be interesting to stay up to date on who is being surveilled and where, but this isn't very nice for the people directly concerned. That's why you should follow the same guideline that applies to militant actions: only those who have something to do with the situation should be in the know.

When You're Under Physical Surveillance...

It makes sense to follow these basic guidelines. Surveillance does not mean the end of all possibilities.

- Surveillance does not normally run around the clock for an extended period of time because it wouldn't be sustainable in terms of personnel. A long phase of intensive surveillance may be followed by a long pause. This means, on the one hand, that a surveillance operation doesn't last forever, but on the other hand, that it can be resumed at some point. Such a pause may last for weeks or even months.
- Or the surveillance may end with a raid, a subpoena, or even an arrest.
- Stay calm. Panicking only benefits the surveillance operators.
- Try to make arrangements with reliable friends who have your back and take on tasks you can't do for the time being. Talk to them, but only to them, and not only about logistics, but also about your fears and insecurities.
- Consider speaking with a lawyer so you already know who to turn to, at least in the event of a sudden arrest.
- To be on the safe side, expect the worst. This means expecting technical surveillance of your home and car, including both camera surveillance and bugs (though this is less likely), as well as tracking devices. You can be sure that your phone and mail are being monitored! Assume that it's not just targeting you, but other people as well. Expect to be detained or even arrested at some point.

As a general rule, you should avoid conspicuous behavior. Don't keep turning around on the street or peeking out the window. Don't engage in any "conspiratorial" activities in an area visible through your windows. And don't make any half-hearted attempts to shake off your pursuers. You should only do the latter if it's absolutely necessary and you're reasonably sure you'll succeed, with the support of other people. Because anything the surveillance operators might find "conspiratorial" will only make you more interesting.

If you politically organize in non-clandestine projects, you and your trusted people need to consider the extent to which you should inform the group. Depending on the structure of the group, not everyone may need to know. Especially if there are inexperienced or less resilient people in your group, you should develop a very precise approach to the situation. Unfortunately, sometimes warnings can do more harm than good, in which case a responsible and considerate response to the situation may be better than verbal warnings. You might prefer to take a "vacation" for a while, or at least withdraw from parts of the group work.

If you participate in clandestine projects, the situation is completely different. You then have to discuss very carefully to what extent these activities could already be endangered by the surveillance that is targeting you, and whether you should pause your involvement, either partially or completely. Conversely, a sudden termination of certain contacts may also appear suspicious. Obviously, the others with whom you organize in this way must be informed of the situation. But clandestine organization does not automatically mean that everyone will be able to cope with the situation. Recklessness, overconfidence (especially among men), insecurity, paranoia, gossip, inaccuracy—all of this is also present in clandestine organizing.

If you have determined that the surveillance you have detected is NOT targeted at you, it's unnecessary to go around telling everyone what's going on. Doing so should only be a last resort when you have no idea who is being surveilled and who you could tell. Otherwise, panic is often created by mixing half-knowledge or assumptions with observations, and people who want to make themselves important run around spreading rumors. It's always better to inform individual people who you can trust

4. Our Security

Traces

Let's start with something important—we don't want this chapter to cause panic! When dealing with the topic of traces, it's easy to get the impression that it's impossible not to leave trace. However, militant actions from the last few years show that a lot is possible, and that successful investigations are actually quite rare. So don't be put off and be careful! Knowing the other side's capabilities and acting with caution are the most important factors to avoid prosecution by the cops and courts.

A trace can be anything, no matter how small or inconspicuous. Every change in the environment leaves traces, so it's impossible to leave absolutely no trace. What's important is to leave as few traces as possible, and to make sure that they can't be linked back to you. To this end, no expense or effort should be spared. Gloves and other action materials and tools should always be bought new, for single use.

The police will look for traces directly at the action site, on any suspects and in the places they frequent (home, workplace, etc.) So it's not enough to only pay attention to traces at the action site—you may also bring traces from the action site home with you. An example is sand or soil —their composition can be analyzed and identified quite precisely by forensic laboratories. So if you bring home mud from a dirt road on the soles of your shoes, this can prove that you walked on that dirt road. Such subtle traces quickly become difficult to analyze. If unlucky, however, there may be enough of a trace left to reconstruct a connection to you, which can then be interpreted as evidence of your involvement in an action. This is even easier with traces of glass or DNA, i.e. anything that doesn't degrade quickly. If you deliberately leave something at the action site, you can be sure that it will attract special attention. The same goes for action claims sent in the mail, or if any remnants of the materials you used fall into the hands of the police.

Securing and analyzing evidence is time-consuming and expensive. The full repertoire of forensic gadgets is not always used. Most of the time, the bigger the damage or the attention, the more they will invest in the investigation.

It's also important to keep in mind that forensic methods are constantly evolving, and methods that were introduced recently are becoming standardized and widely used. Precautions that we consider excessive today may not be sufficient in the future. A good example of this evolution is DNA analysis. Thirty years ago, hardly anyone foresaw this relatively new investigative method, which naturally meant that minimal precautions were taken to avoid leaving DNA traces. As the example of federal prosecutor Buback (who was shot dead by the RAF[1] commando Ulrike Meinhof in 1977) demonstrates, with the right political pressure, traces found decades earlier can be re-examined. In this way, the State shows that it doesn't forget, and perhaps also tries to deter today's militants.

In addition to the problem that old traces can eventually be analyzed using new methods, these new methods can become increasingly widespread and less expensive through their further development and standardization. The threshold is lowering for using DNA samples as evidence in increasingly petty crimes on the basis of vague suspicion. The amount of genetic material required for analysis has also been reduced.

Specific laws could also be overturned, such as the ban on storing information about certain physical characteristics or diseases in the databases of the BKA[2] and LKA,[3] since they already allow storing information about genetic sex.

Of course, we can only present the topic of traces in the context of today's forensic methods. But we think it's important to take into account the constant development of these methods, even if we can't foresee it.

[1] *N.T.P. note:* Red Army Faction, a West German far-left militant group founded in 1970.

[2] *N.T.P. note:* The Bundeskriminalamt (BKA, *Federal Criminal Police Office*) is the federal investigative police agency of Germany.

[3] *N.T.P. note:* The Landeskriminalamt (LKA, *State Criminal Police Office*) is the State-level police agency of Germany.

these matters. Most importantly, you need to work with your own people to figure out what works for you and what doesn't.

What You Can Do

There are various ways you can behave: you can continue to live as before and, if necessary, temporarily refrain from doing risky things. In doing so, however, you accept that the other side will learn a lot about you, your social contacts and your political connections. The advantage of this approach is that you can largely ignore the surveillance. But to protect others, you must consider where you could be taking the surveillance operators with you and who they might become aware of because of it.

Another approach is to put your political life on the back burner, so to speak, by lying low and waiting until the other side gets bored or finds the surveillance pointless because they simply don't have anything interesting to see. But keep in mind that they may have been watching you for longer than you know, and could therefore notice if your life suddenly changes.

Alternatively, you can go on the offensive and "burn" the operators who follow you by openly addressing them, taking photos, or the like. Perhaps you could turn this against them with an appropriate political campaign and publicity, but you also run the risk that this will draw real attention to you. Maybe they'll wait a while and then send a better team against you that you won't notice so easily. In this regard, you should consult with others before deciding to take this approach. It's tempting to show the operators that you've detected them and to tell them to go fuck themselves, but you'll probably be trading a short-term sense of accomplishment for the long-term ability to have control over the surveillance operation.

In any case, it may make sense to get a lawyer involved. Here too, you need to think about what you should and shouldn't tell them. Of course, lawyers can't work miracles, and they usually know a lot about legal matters, but not necessarily about cops or intelligence agencies.

What Could Be a Threat in the Future?

Based on your working hypothesis of what the surveillance is about, you can consider how the authorities will proceed. One unknown factor, of course, is whether it's the cops or an intelligence agency that have you in their sights. If it's the cops, it's very likely that you are the subject of an investigation, which will usually be related to "§129" or "§129a".[31] It should be briefly mentioned that these two articles are primarily investigative in nature and are used to keep the repressive apparatus running smoothly. Very few §129a investigations lead to trials and convictions. They are mostly used to legitimize surveillance in the first place. So a §129a surveillance operation will not necessarily be followed by a raid and/or arrest. And if it is, this does not necessarily mean that you'll be charged. You should familiarize yourself with this possibility, but it's also possible that the surveillance will end at some point and nothing concrete will result from it, except that your file with the security or intelligence agency will be a little thicker.

The intelligence agencies are not formally subject to the principle of legality, i.e. they can surveil you "if necessary" as they wish. Whether anything else follows from this depends on whether the intelligence agency activates the police.

If the surveillance lasts for months (which can happen), you can't live with your bags packed the whole time, whether it's to run away or to go to jail. You have to find a routine for yourself at some point in this situation, otherwise you'll lose it. This means that you either have to give up certain things during this time, or you have to arrange them in such a way that you can carry them out despite the ongoing surveillance.

Some people have lived for years under the constant threat of surveillance and have continued their political activities. But they are unlikely to publicly discuss many of their experiences during that time, so as not to give the cops any clues as to how they managed to make the surveillance go nowhere. Therefore, if you are affected you will have to do a lot of research yourself or seek direct contact with comrades who have experience with

[31] *N.T.P. note:* The terms "§129" and "§129a" refer to paragraphs in the German penal code that deal with the formation a criminal and terrorist association, respectively.

New methods are often considered, discussed, and tested before they are actually used. (The fact that they are then used before they are legalized is another matter…) So we think it's important to keep an eye on these developments and keep each other informed by discussing them in our publications.

Phones and the Internet are not discussed in this chapter. But just briefly, we think it goes without saying that phones should not be involved in actions or their preparation. They can be used to create movement profiles as well as turned into bugs. They are full of information about you and your contacts. Every click on the Internet leaves several traces on the computer you are using, on the server you are accessing, and on all the servers in between. Some of these traces can be avoided or controlled, but that would be a whole other chapter.

We cannot provide a complete list of possible traces here. So it's important that you think through all the steps yourself and consider where you may leave traces.

The fact that there is no such thing as 100% security is used by the police to portray themselves as omnipotent. The evidence gathering process and forensic investigations also have a psychological function. The point is to use the gathered evidence to convince you that you're already found guilty. This is how they extort confessions. Even if the evidence is clear, it is often only circumstantial and not proof of your involvement in the crime. A conviction usually requires more than just circumstantial evidence. So even if the cops charge you and claim they have enough evidence against you, stay silent during all interrogations!

Fingerprints

Fingerprints are a criminology classic. They come from the thin layer of acid, grease, and dirt from our fingertips which is left on objects we touch. Police also record the prints of the entire hand, including the palm. Fingerprints are considered unique to an individual. When you are charged with a crime, it's standard procedure to have your fingerprints taken for comparison. They are still often taken with ink and paper, but scanners that digitize them directly for storage in the relevant databases

are becoming increasingly popular. Meanwhile, the State has already turned its attention to the new passport production process which makes it mandatory to provide fingerprints in order to obtain a passport. It remains to be seen how this will affect police practice. Fingerprints are stored in databases called AFIS (Automated Fingerprint Identification Systems) in order to compare prints from current and past cases.

The best remedy for fingerprints is to consistently avoid leaving them. This means not touching any objects that could fall into the hands of the police with your bare hands to begin with, rather than relying on cleaning them off. Fingerprints are one of the most durable traces. They are often left carelessly and can persist for years. Even on objects that have been submerged in water for years, fingerprints can still be recovered under certain conditions. Almost any material can bear fingerprints.

Other countermeasures exist. To remove fingerprints, thorough cleaning with a degreasing agent (such as an alcohol-based cleaning agent) is recommended. Glass and smooth plastic surfaces are the easiest to clean; it's enough to thoroughly and intensively clean and wipe them with an alcohol-based cleaning agent or, if used thoroughly, dishwashing soap. When removing fingerprints from metal surfaces, it is imperative to use a surface-altering agent such as steel wool. Fingerprints are slightly acidic, so they etch into metal. Cops can make them visible again with the help of a laser, depending on their motivation. Scratching the surface with steel wool or sandpaper is one of the best options. Unpainted wood can be treated like metal. Painted or coated wood can be treated like plastic surfaces. Although fabrics are poor carriers of fingerprints, they can be identified by their unique composition, and they also carry DNA. Be careful what you leave behind at the action site!

If you have touched a piece of paper with your fingers, you should make a clean copy then destroy the original, as it's impossible to clean it. When photocopying, you should make sure that you never directly touch the copies with your hands. Since it can attract unnecessary attention to wear gloves in a copy shop, you should simply make a few blank copies before and after the pages you want to keep clean. Then touch the stack of paper only from the outside and place it in something like a new folder. Don't use a copy shop where you are known. Use disguises because it

develop a “nose” for cop cars, since it's usually impossible to remember the license plates of all passing vehicles.

Once you have confirmed that the surveillance is indeed targeting you, you need to calmly consider your next steps. You shouldn't do this alone, but with a few people you trust.

Who and What Is at Risk?

Regardless of why they are tailing you, consider whether there are any other comrades who might be affected. They need to be told, but it may be better if this isn't done by you personally.

If there are things that could be a problem in your home, car, or other places where you spend a lot of time, they should be discreetly moved elsewhere.

First of all, don't tell more people than absolutely necessary. Once rumors of surveillance begin to spread, the most likely outcome is panic, anxiety, and conspicuous behavior, as well as speculation about the possible reasons for the surveillance. All of this can do more harm than good.

What Could Be the Reason for the Physical Surveillance?

To get as close as possible to answering this question, collect as many observations as possible: dates, times, vehicles. Distinguish assumptions from reliable observations. Then try to come to an assessment of what the surveillance operators (could) have already noticed. Think about all the possible reasons for their activities. Don't just think about your real activities and struggles, but also about what is conceivable due to coincidences or unintended connections. For example, if you have been identified by the police when you were with someone, such as in a previous arrest. What type of vehicle were you using when you detected the surveillance? When and where did you do things that could be understood as conspiratorial activity?

will then position themselves as inconspicuously as possible along the route you will take at the specified time. They record exactly when you pass by and what follows behind you: the car's license plate, color, model. The observations are then compiled. If you are really being surveilled, the fact that the same people or cars were seen in different places will serve as confirmation. However, it's more likely that your friends will immediately recognize the surveillance operators, because to keep up with you they often have to race through the streets at high speed and disregard traffic laws. The most important thing for the operators is to keep up with you without being seen by you. This leaves little room for consideration of other road users.

Of course, there's always an element of uncertainty. It could be that you have a tracking device on your car, and that's why the surveillance operators kept their distance (but they're still tailing you!). Or they were following you, but then lost you. Or they finished work or took a lunch break a few minutes before you started your route. That's why counter-surveillance can only ever reveal if they were tailing you at that particular point in time. Nevertheless, if you choose the time and place well, you have a good chance of getting enough certainty for your immediate plans.[30]

You can also try to detect surveillance by yourself. Take a carefully planned route by car or bike that gives you the following options: you can make surprising turns—preferably with a plausible explanation. Or you follow a long, straight stretch of road with no turning options, where you can suddenly stop on the side of the road. In both cases, your pursuers will be forced to pass you if they don't want to attract your attention. You can then try to memorize cars, license plates, and faces, and repeat the whole process elsewhere to see if there are any matches. In order to carry out surveillance detection measures, however, you must be able to behave in such a way that the cops don't notice what you're doing. Above all, this requires you to remain calm even in a tense situation. You must also

[30] *N.T.P. note:* For more information on conducting counter-surveillance (i.e. detecting physical surveillance with the help of a trusted third party), see Surveillance Countermeasures.[a]

[a] https://notrace.how/resources/#surveillance-countermeasures

may be possible for the cops to trace which specific copier was used (the same applies to laser printers, see Writing Traces, p. 18). Copiers can store information on what they've copied, and this information is not overwritten by making a few additional copies.

Gloves are the simplest and safest way to avoid fingerprints. But there still are a few things to keep in mind—rubber gloves tear easily, and fingerprints remain on the inside and on the cuff. Thin latex gloves can even allow fingerprints to pass through them. One option is to wear two pairs on top of each other or to use dishwashing gloves. In contrast, fabric gloves have the advantage of being difficult to leave fingerprints on. But coarsely woven fabric gloves can get holes, especially with repeated use, and thus should be avoided. Fabric gloves also absorb much more dust and DNA traces than rubber gloves, and are virtually impossible to clean. Leather gloves are relatively expensive and, as with all gloves, must be disposed of after use. This is a significant disadvantage in our opinion. In general, keep in mind that traces remain on the inside of gloves. In our opinion, gloves that have been used during an action should always be disposed of. This is because traces that remain on the gloves which can be linked to a specific action. Gloves also leave traces of their individual profile or minor irregularities at the action site (see Material Traces, p. 20). During house raids, cops are often particularly eager to find such equipment.

There are other ways to avoid leaving fingerprints, especially when wearing gloves is not an option. One is to apply a thick layer of liquid bandage to the fingers and let them dry. Another is to place regular band-aids around or on the fingertips. We do not consider either of these methods to be particularly secure, they are just a way to reduce the amount of traces.

A new method currently being tested in the U.S. makes it possible to analyze the chemical composition of fingerprints. This analysis makes it possible to identify and detect drugs, explosives and certain metabolic products, and draw conclusions about possible "perpetrators." The analysis process is fast and can be done directly on site. Although it has not yet been used as evidence, it's only a matter of time.

DNA Traces

In recent years, DNA traces have become an increasingly important part of dealing with repression. The repressive apparatus has a strong interest in emphasizing both their inevitability and their lack of ambiguity.

It's true that DNA traces can often only be avoided with significant effort and that they are almost impossible for us to detect due to their near invisibility. And they are often considered irrefutable evidence if found at a crime scene. How these traces got there is often hardly taken into account. For example, a blanket used to cover a tool can carry the DNA traces of someone who slept under it years ago.

DNA traces cannot be avoided, and under certain storage conditions they simply do not degrade. Decades after the fact, cases are being reopened based on DNA evidence collected earlier. DNA traces are left behind by blood, hair, saliva, urine, and skin cells. In other words, everything that comes out of your body or falls off it. But not every trace is sufficient for a DNA comparison. Laboratory testing still requires a certain quantity of DNA material, preferably one or more intact cells. But the technology is becoming increasingly sophisticated.

DNA analysis is expensive. This means that it's not ordered in every case. Generally, the greater the political or economic damage, the greater the technical effort. Though this may change in the near future. Cheaper tests are being researched and DNA analysis may become the standard. DNA databases have been filled for years.

It's relatively easy to determine genetic sex using DNA. To be able to analyze the trace beyond that, the police need a comparison sample from you. Such a sample is either obtained during an ID check or from personal items such as a comb found at your workplace, during house raids, etc. There have also been instances of police forcing relatives of defendants to give samples because their DNA is similar. You should never give samples voluntarily. Protest and object, don't sign anything! In some cases, it has been possible to prevent or at least delay the submission of DNA samples with the help of lawyers.

3. What To Do if You Detect Physical Surveillance

If you are certain that you have detected surveillance, you will naturally want to know whether it's targeting you. If there is no evidence to the contrary, you can try to find out more by conducting "counter-surveillance." To do this, you need a few trusted people who can be observant. Decide on a route that you will take at a certain time. This route should be designed to fit in with your daily routine so that surveillance operators don't become suspicious. It should have a few turns to rule out coincidences, such as a car that happens to be driving the same route as you. It doesn't have to be particularly long. It should not follow the main traffic routes all the time, but it also shouldn't circle around itself too much, otherwise the surveillance team may simply form a box around it. Short stops can be incorporated to make sudden changes of direction plausible. For example, first you go to a copy shop and copy something, then you turn in the opposite direction and go to a mailbox where you drop something off. Then you can change direction again and buy a newspaper at a store. It's best to do the route in a car, because then you will be followed by vehicles and not on foot.[29] It's easier to describe vehicles more precisely than people. Since you want to determine whether someone is tailing you, it makes no sense to try to lose potential tails. You should also avoid checking yourself, as others will do that for you. Your pursuers should feel as safe as possible.

You must communicate your chosen route to your comrades in advance. If it seems too risky to meet them in person, you'll have to find another way to communicate the details. However, the easiest way is to tell the route to people you can meet without issue or raising suspicions, and who are very unlikely to be under surveillance themselves. Your friends

[29] *N.T.P. note:* If you do the route in a car and you are under physical surveillance, there is a risk that the car contains a GPS tracker installed by the surveillance team to track its location. This is a problem, because the surveillance team might rely on the tracker and follow you from far away or even not at all, making it harder or impossible for you to detect them. It can be better to do the route on a bike, because compared to a car, it is easier to ensure that a bike does not contain a GPS tracker. For more information about using bikes, see our Threat Library's "Transportation by bike"[a] mitigation.

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

If you think you've detected surveillance, the second step is to determine the surveillance target. To find out the location that is under surveillance, you can either look for it directly, i.e. look for an operator watching a specific location, or you can think about what is likely to be surveilled in the area and then try to detect an operator around those locations. If you don't find the object of your desire, there's not much you can do other than walk around attentively for a while. Without identifying the target, it's not possible to draw conclusions. Accordingly, you should limit yourself to making sure they are not targeting you or people or locations you know.

If you can detect the trigger position, the next step is to determine what the trigger is watching. Although you know the target must be a certain distance away, you don't know if it's a house, a car, or something else. For example, the target could be a car that is parked 100 meters away, but which can nonetheless be seen from this distance if it drives off. You can first try to rule out possible targets. Rule out all properties in the immediate vicinity of the trigger position, i.e. the two to three adjacent house entrances, pubs or shops. Keep in mind that it's also possible for a trigger in a car to use the rear-view and side mirrors. Despite these clues, it's very unlikely that you'll be able to determine the exact target location. At least you can narrow it down to a certain area and, above all, you can assess whether your own front door, car or bike, or those of your comrades could be affected.

If you come to the conclusion that your own front door is in the line of sight, your adrenaline level will probably skyrocket, but stay calm. So far, nothing is confirmed, and many other possibilities exist. However, if you cannot rule out surveillance of your front door, it makes sense to take certain precautions. For example, are there people you don't want seen entering your home? Do you keep things at home that you feel uncomfortable with in such a situation? Would you prefer not to be identified as someone who lives there? So you need to start thinking about what to do: ignore the danger, warn people, take countermeasures? That's what the third section is about.

Since it's difficult to avoid leaving DNA traces, it's important to minimize them. This starts with not taking a piss near your target or leaving a cigarette with spit on it. It's best not to smoke at all during an action.

Avoid hair traces by wearing caps and balaclavas. Long sleeves, even in summer, reduce the amount of skin particles and small hairs that fall off. A face mask helps against saliva and nasal mucus.

If you bring tools and bags with you that you have previously stored at home, make sure they are free of not only fingerprints but also hair and skin cells. They can very much carry DNA. The same goes for your clothes and shoes. It's best to keep everything you bring to the action separated in clean containers, such as unused garbage bags. You should avoid storing important action materials at home. Hair from your pets can also be traced back.

Action claims sent through the mail are often examined for DNA traces on the paper, the envelope and the postage stamp. Saliva on the adhesive surface of envelopes is particularly easy to analyze because it doesn't degrade. When producing anything that could fall into the hands of the police, such as letters and the remains of your action materials, you should always minimize the risk of leaving DNA traces.

Options for Creating a Clean Room

For certain tasks, it makes sense to set up a “clean room” that is more or less free of DNA. This room's function is both to minimize the traces you might leave on an item and—to the greatest extent possible—to minimize leaving traces in the room itself. This is certainly time consuming and not inexpensive, but ultimately you have to make your own decisions about how secure you want to be. When weighing security precautions, consider not only the intensity of the action, the motivation of future investigators, and your own security needs, but also the likelihood of an action item falling into the hands of the authorities. For example, you can be sure that letters sent to the press will end up with the police sooner or later.

The following description may seem extreme to many, and certainly not all of the following precautions are necessary for every action. However, in light of the rapidly developing field of DNA analysis, we think it's important to be aware of the issues and risks involved. Choose the precautions you feel are necessary for your action and don't be deterred!

To set up a clean room, you'll need to put on protective clothing before entering the room for the first time to avoid leaving DNA traces in the room. You can use coveralls (still in their unopened packaging!) from the hardware store, which are relatively inexpensive. Put them on and also put on an unworn balaclava—pull the hood of the coverall over it. Bathing caps are also good for covering your hair, as they are even more impermeable and your hair won't be able to poke through. Next, place each foot in a garbage bag and tape the bags to the legs of the coveralls. Then put on rubber dishwashing gloves and tape them to the sleeves. If possible, put a mask over your mouth to block droplets of saliva, and put on protective goggles that also cover your eyebrows. Always work in pairs and make sure no skin is exposed.

Choose a place to work where your hair and skin cells are not already flying around. It should also be free of hair from a dog, cat, or other animal companion that could be classified as your pet. For example, use the basement or garage of friends (who are not politically active), or rent a hotel room. Set up a clean work surface, preferably with a tarp, or if you want to be on the safe side, set up an unused tent in the room. This tent will at least keep most traces of your work inside, and you can dispose of it securely afterwards.

When you work, you should have different garbage bags ready and separate the waste according to how risky it is for you (e.g. waste from a device component in a bag, the Ziploc packaging in another, etc.) When separating waste, you should also consider which packaging has your fingerprints on it and which doesn't. Obviously, none of these garbage bags should be put in your household trash.

Be aware that working in these clothes is both sweaty and tiring, and consider relieving each other or sharing the work if necessary, as interruptions will require you to change clothes again. Remember not to scratch your head or face while wearing gloves. For example, a good

comfortable and less visible from a distance. Or they may do something to give themselves a reason to be there, such as reading the newspaper. The trigger position can also be done on foot. In this case, someone may sit in a cafe with a view of the target's front door and only briefly signal to the rest of the team that the target has left the house.

If you see a car with one or two people sitting in it, looking intently in one direction, you can be relatively certain that you have found the trigger position. Unless it is well camouflaged, this position will normally be at a distance that gives a good view of the target, but is out of the target's immediate field of vision. This is usually about 40 to 80 meters.

The rest of the surveillance operators are at some distance. However, they still need to be close enough to be able to start tailing quickly when necessary. So they will make sure that they are well positioned in terms of the street layout and that they can quickly reach the target's possible routes. They are probably around a corner or two, about 200 to 400 meters away. If they take a more relaxed approach, they may gather in several cars, perhaps even getting out to chat. However, they may also line up separately and form a box around the target. They also need to find places where they can meet and discuss undisturbed, such as dead ends or parking lots.

The cars will change positions occasionally. The car that was in the trigger position joins the stand-by cars, and another car assumes the trigger position. If finding a parking space is difficult, the first car waits until the car replacing it arrives and then leaves the parking space to its replacement.

The following are signs that surveillance may be taking place:

- Have you seen people staring at a fixed location?
- Have you seen people wearing earbuds?
- Have you seen occupied cars parked for several minutes?
- Have you seen cars (moving or parked) that you suspect are surveillance cars?
- Have you heard radio transmissions from cars?

gotten out of a car. Cars have several advantages for the cops: they can hide their radios and other equipment (a camera, a change of clothes) in the car. They can speak loudly and listen to radio messages without being noticed by outsiders. They can move between locations quickly. They can sit comfortably and maybe even take a nap if the surveillance drags on without much happening. Of course, there are also operators on foot, bike, and motorcycle, who are usually harder to spot.

Surveillance vehicles are generally clean and well maintained. There are all kinds of car models in all kinds of colors, mostly high horsepower models, but no souped-up or otherwise flashy models. Don't expect to see any technical features like radios, radio antenna or anything like that. Gone are the days where surveillance cars gave that away. Nowadays, the cars have "hands-free" systems where messages are picked up by a hidden interior microphone and the radio can be hidden in the glove compartment.

So if you're out for a walk, you might pass a car that catches your eye. You take a closer look out of the corner of your eye and see that the car is clean, it has an antenna, someone is sitting in it reading a book. Other than that, the car looks normal. Or there are two people in it with their seats partially reclined, maybe dozing off. Or someone is just sitting there looking intently in a particular direction. Or maybe you just see a man or woman with headphones standing idly on a corner. Shortly thereafter, a car slowly rolls past you with two young men in it, looking out the window with interest. Then, two corners further on, two cars are parked next to each other with two couples standing next to them, smoking and chatting. They are probably wearing normal, sporty, casual clothes and shoes. They don't have "cop faces," nor do they look particularly strong. But maybe you heard a beeping sound coming from one of the cars as you passed by.

You may have just noticed the two essential elements of surveillance: first, the "trigger" position for the target, and second, the surveillance operators that stand-by ready to tail the target.

The trigger position is of central importance, which is why it must be particularly inconspicuous. If this position is occupied by people in a car, the surveillance operators may recline the seats to make themselves more

division of labor is to have one group prepare the clean room and another group enter it to work. Store finished components or items in new freezer bags or Tupperware containers.

When you put on protective clothing, and at every step of the process, think about what items your DNA traces may adhere to. For example, if you bought something in packaging, you probably handled it without gloves so it may have skin cells on it. If you touch the packaging with clean gloves, you can transfer DNA from the packaging to the gloves and from there to the items you're working on. To avoid this, you must work with a lot of discipline and change your gloves several times, which is easier to do if you wear a second pair of gloves over the taped gloves.[4]

Artificial DNA

Artificial DNA is a new method of deterring and prosecuting theft. It may be less relevant for the radical left at the moment, but who knows what the future holds? Like human DNA, artificial DNA is unique and uniquely identifiable. It is placed in an adhesive carrier liquid that glows purple under UV light, along with equally unique micro-platelets. The substance can be applied to valuable objects with a brush, or buildings can be equipped with so-called DNA showers. The marking on objects is permanent and resistant to normal cleaning. If you come into contact with the substance, it will stick to you for about six weeks. This relatively new process was introduced as a pilot project at the end of 2009 at schools in Bremen, Germany, in two residential areas and in some petrol stations. It has been used in the United Kingdom and the Netherlands for some time.

Scent Traces

A more recent development is the collection of scent samples, as was done during the raids on militants suspected of opposing the Heiligendamm

[4] *N.T.P. note:* For more information on creating a clean room, see "DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces".[a]

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

G8 summit in 2007. Although these are rather dubious, even according to the BAW,[5] they could contribute to an "overall assessment". Most importantly, they are easier to obtain than DNA samples.

According to scientific findings, every person has a unique and unmistakable scent. Even the most meticulous cleanliness and hygiene cannot prevent this scent trace, known in technical jargon as a "human scent signature."

It is made up of various components, but mainly of decomposed skin cells. People shed these every second, whether they are sitting, walking or standing. The decomposition of skin cells by bacteria produces gases that can be detected by sniffer dogs with their highly sensitive noses. The goal is to match body scents with scent traces that have been left at a crime scene.

Shoeprints

Shoeprints are an often underestimated potential danger. They are as individual as fingerprints and can be used to draw conclusions about the height, weight, gait, etc. of the person who left them. If the shoe that left the shoeprints is found during a house raid, it can be identified with relative certainty, depending on the quality of the prints. Traces of soil or plant residue left on the shoe will do the rest. It is therefore advisable to dispose of your shoes after an action, especially if you have walked over snow, soil, etc.

However, shoeprints don't depend only on the shoe's model, but also on the way it's worn. All shoes worn by the same person will show the same type of wear. If shoeprints are left in soil or snow, the police can make a plaster cast from it. Using this cast, they can often not only identify the shoe that left the print, but also match other shoes worn by the suspect to the cast based on the specific wear patterns found on the cast. So don't use old, worn shoes of yours, especially if you have to walk on soft surfaces.

[5] *N.T.P. note:* Bundesanwaltschaft (BAW) is a name given to Germany's federal prosecutor office.

so we think they don't know anything…" or "They struck now because they knew everything beforehand…"). This happens sometimes, but the reasons are usually far more mundane.

So, try to get to know your adversaries. Describe not only their logic (or lack thereof), but also what they look like, how they act. The days when 95% of surveillance operators were men with short hair and mustaches are long gone. Today, there are many women among them. Both women and men wear clothes typical of the scene, and the men often have long hair and earrings.

How do they sit in the car? Why does a surveillance operator look out the car window differently than other people? He or she is looking out for something. However, it's easy to mistake people who are unfamiliar with the area for surveillance operators, because they are often very alert. Most people who drive tend to focus their attention inside the car, especially when they're not alone. Surveillance operators, on the other hand, usually pay close attention to their surroundings outside the car and often hardly talk to the other passengers.

In any case, it makes sense for anyone who is politically active to consider the extent to which they should prepare for repression, to become more familiar with the possible threats posed by surveillance, etc. Do not rely on the fact that from time to time, some license plates of surveillance cars are published somewhere. The lists can contain errors, the license plates are changed. The best protection is to develop a "nose" for cops and informants, and you will develop this through attention and experience.

2. How To Detect Physical Surveillance

Let's assume you're up to something so you want to go scope out an area. Or you have nothing to do at the moment and are taking an attentive walk. How can you detect whether there is a surveillance operation going on?

Cars are the most noticeable element. For once we can be happy about the car society we live in. Cars are easy to identify and can be clearly described by their model, color, and license plate number. Almost all stakeouts involve cars, and the operators on foot are usually passengers who have

should first ask yourself how this feeling relates to your political activity, and whether you can afford such an approach to this activity. If you can, great, if not, you need to think about how you can find a tolerable way to deal with it and to what extent others can help you.

The police and intelligence agencies are always present in one form or another, without this necessarily resulting in anything concrete. There's a good reason that it's common knowledge that informants should be assumed to be present at every public meeting, that phones are tapped, etc. In fact, this has never successfully prevented radical left action.

Despite its rules and laws, the security apparatus is not completely predictable and certainly often a bit chaotic. They may not even know themselves what is going on at the various levels.

General caution means being aware of the cops' presence and not being deterred by it. After all, an essential element of "preventive repression" is to create paralysis through a general awareness of the constant presence of the cops. This is intensified by police games designed to keep us occupied —seemingly pointless or untargeted blows of the repressive apparatus are sometimes simply meant to keep people busy so that they don't have time for anything else. When this is the dynamic, the cops have the initiative. They're on the offensive, and we're chasing after events. This political aspect of repression has been extensively discussed in other texts.

General caution means paying attention to how cops behave. Sometimes it can be useful to imagine how and what they think: the patrol cop, the surveillance operators, the State security cops, the chiefs. Surely they're not only thinking about us and our "misdeeds," but also about the end of the day, their mortgage payments, their boss, the political repercussions, their career, the union, getting something to drink later, the arrogant external authorities. It's important to consider that what they imagine of your daily life is shaped by the mass media, biased informant reports, difficult-to-comprehend texts from the scene, and lectures by "scene experts."What are their moral values and self-justification for their work? If you go beyond the sloganeering notions of cops as recipients of orders without agency, or as fanatical law-and-order fighters, you will no longer be surprised by some things that you might not otherwise be able to explain without enormous conspiracy theories ("They didn't intervene,

If you really want to be sure, buy cheap shoes just before an action and throw them away afterwards. However, there are bound to be DNA traces on shoes you used, so never dispose of them near the action site.

Another way to make the cops' job more difficult is to wear socks over your shoes. This disguises the model and profile of the shoe and can also protect against video surveillance. But before doing this, try walking and running with the socks on.

Vehicle Traces

You should think carefully about the type of vehicle used during an action. Think about whether a car is really necessary, because it brings many risks.

Cars leave behind tire tracks and, in the event of an accident, traces from the car's paint. Traces (especially paint) from an accident can be found both on the car and at the scene of the accident. Tire tracks and paint chips can be used to determine the car's model, and if the car is found, to determine whether the traces were left by this car specifically. Changing the tires, if possible both before and after the action, can make it more difficult to identify the tire tracks. Simply changing the tires after the action is not enough, as the police may be able to compare the tire tracks found at the action site with tire tracks outside your home or in your garage. Also, when using a car, watch for leaking oil or fluids.

But by far the most important identifying feature of a car is its license plate. In order to pass at least one license plate check without being pulled over, the car's license plate can be swapped with another. Since most of us aren't able to manufacture license plates, you can steal them just before the action. It's important that the car from which you steal the plate is the same model and color as the one used in the action, because, as a standard procedure, cops check the license plates of cars and know whether they have been reported stolen, their color and model. If the car hasn't been reported stolen and has the correct model and color,

the likelihood of being pulled over is somewhat reduced.[6] Stolen license plates will however not pass a proper vehicle inspection.

To prepare for the risk of a vehicle inspection, you should hide your action materials well and, if possible, not in the obvious location of the trunk. Make sure the vehicle meets all legal standards. In Germany, don't forget your legally required warning triangle and first aid kit.

To remove a license plate, a screwdriver will usually do the trick. Try this for the first time in a quiet place where you can work without stress. After unscrewing it, you can use double-sided tape to attach the license plate to your car (watch out for rain) so it's easy to remove after the action.[7] Alternatively, you can smudge or mask license plates, especially on motorcycles, but this is conspicuous. Dealing with the license plate is also important for countering the increasing surveillance by toll and traffic management systems. Toll systems are sometimes used for Automatic License Plate Recognition.

Be aware of the risk of leaving traces in the car and try to avoid this, e.g. by packing the action materials well. In our opinion, it is almost impossible to avoid leaving DNA traces in the car. Not only is a car a good carrier of traces, but it is also easy to track if a covert location tracker has been installed on it. The use of a car should therefore be avoided whenever possible.

Bikes can be a good alternative. They also leave tire tracks behind, which is often overlooked. We therefore recommend that you do not park the bike in the immediate vicinity of the action site. Depending on the surfaces, it may be a good idea to change the tires before and after the action. Individual features such as brand stickers can be easily covered with tape.[8] A brightly colored bike can easily be an eye-catcher. As with

[6] *N.T.P. note:* If you steal a license plate from a car, you can replace it with another, random license plate (that cannot be traced back to you). This way, it might take longer for the car owner to notice the theft and report the license plate as stolen.

[7] *N.T.P. note:* Rather than tape, we recommend using a "magnetic license plate holder" to attach the license plate to the car.

[8] *N.T.P. note:* Covering features with tape is not ideal, as a taped up bike can look conspicuous. In addition, many bike features (e.g. the model and shape) cannot be concealed with tape. One solution is to steal a new bike for each action and dispose of it afterwards.

Of course, there are also clues that you can use to determine how much the cops know. You can for example determine which of your friends are also being surveilled, or at what times they surveil you. If they always come in the evening, they probably aren't watching you for organized shoplifting at the grocery store.

Paranoia Feeds on Itself

Once you've detected signs of surveillance around you, you may start trying to deduce meaning from the smallest things. Suddenly you suspect cops around every corner, everything is suspicious. This is completely normal, it comes and goes in phases, and also depends on your mood at the time. Try not to let it drive you crazy. Until you become quite "familiar" with this situation, you have to expect that you will not even notice the majority of the surveillance operation, simply because they are careful to keep their distance from you. So if you are absolutely certain that there are cops buzzing around you, it may be a sign that you aren't the target.

What You Can Do Specifically

Now to the practical part, which has three sections:

1. General caution
2. How to detect physical surveillance
3. What to do if you detect physical surveillance

1. General Caution

If you are part of the radical left and politically active, or if you associate with people who are, it can't hurt to be a little vigilant in life. You have to establish your own limits: where does recklessness begin, and where does paranoia? Some people have a nose for cops, others don't even notice when a police radio beeps right next to them. You have to figure these things out for yourself. Your vigilance has to be integrated into your daily life, into the way you perceive your surroundings. If you can't deal with repression at all, if you just want to keep it away from you, then you

Your Enemies Don't Necessarily Know Everything You Know

You may wonder why you've never been put under surveillance. Or you're being tailed and wonder why they are staking out one place and not another. For example, you notice that the cops have been lingering outside your legal address for days, even though you thought they should have known by now where you actually live. But maybe only the intelligence agencies know this, and they haven't told the cops.

You have to be prepared for the fact that if you are a target in a surveillance operation, you won't be surveilled in the same way that you would do it yourself. They don't know a lot of things that you know. But they also know things you don't. Or they can be wrong and start from a completely false premise, like associating you with someone you have nothing to do with. Another possibility is that they are working on a construct that is politically desirable, but has little to do with reality. So you shouldn't assume that the surveillance is based on what you know, or even based on reality. Your adversaries are working on the basis of what they have in their files, and these can be quite inaccurate.

If you automatically assume that they know what you know, you may then deliver this knowledge to them through your behavior. If you suddenly start moving boxes out of your apartment because you've become nervous after detecting surveillance, you may be letting them know that you actually have something to hide.

Of course, the first question during a surveillance operation is always what they are actually interested in. Don't expect to find out! If you know that a “good” reason exists to target you, then assume that is the reason. But you must also expect that there could be reasons you would never think of. For example, you may have unwittingly sold your car to someone who is under surveillance for organized car smuggling. Or when a person accused of being a member of the RAF was arrested, they found a piece of paper with a number on it that the BKA mistook for your phone number. Or a snitch falsely accused you of having contacts with a clandestine militant group. These are all things that no one will probably ever tell you, so you won't be able to evaluate them.

cars, it is important to meet the legal requirements for bikes, especially when you are out and about at night.

Tool Traces

There are many ways that tools can leave traces, and each tool is different. Therefore, we can only write a few basic things about the topic here. By tool traces, we mean identifying traces on both the tool and the object the tool is used on.

Each tool is unique and can be identified through both small irregularities from its production process, and normal wear and tear. Each tool leaves unique traces on the object it is used on. For example, a cut sheet of paper can be matched to a specific pair of scissors (only if the cops have the scissors, of course). If the cops do not have the tool in their possession, typically only the type of tool can be determined, at least for mechanical tools which come into direct contact with the object the tool is used on.

Therefore, you should dispose of bolt cutters, screwdrivers, or whatever else is used in an action—get rid of any tool that came in direct contact with an object it was used on. Unfortunately, getting rid of the tool afterwards is not enough by itself. To stay with the scissors and paper example, the cops can not only match the cut paper to a particular pair of scissors, but also determine if separate pieces of paper were cut by the same scissors. So if you open a fence with the same bolt cutters you used to build your loft bed, the cops will be able to determine this, even if the tool is long gone.

This is why it's necessary to acquire new tools for an action in order to work securely. They don't always have to be the best and most expensive.

Consumables such as tape, rope, cable (and their remnants) can be matched to each other. A small piece of cable in your home that matches a cable in the cops' possession can be a strong piece of evidence.

When working with either tape or glue, you need to be especially careful about cleanliness, as both collect dust and DNA traces.

Identifying traces can also be found on tools you make yourself, such as an incendiary device. Such traces are not limited to DNA or fingerprints. For

example, to determine whether the same person made separate incendiary devices, it's often sufficient to examine identifying characteristics of the way the devices were constructed. Everyone interprets and implements a general, simple set of instructions differently. For example, everyone ties knots in a particular way, tapes something differently, uses a different construction method, and so on. The list does not end there and identifying characteristics cannot be completely avoided, but they can be reduced if you are aware of them. Even taking turns within the group to build materials for the action makes it harder for cops to attribute them to a specific group or person—this is even more relevant if an incendiary device fails to ignite.[9] Additionally, sharing the task of building materials prevents unnecessary specialization within your group.

In the self-critical dissolution statement of the K.O.M.I.T.E.E.[10] published in 1995, they wrote that the cops were only able to easily attribute some actions to them because they always used the same type of igniter for their incendiary devices. So the decision for or against variation in device construction has to be made consciously and contextually. This also applies to possible variations in the chemicals used for an action and, as far as possible, their mixing ratios. Similarly, you should not always use the same brands or component types. In general, the simpler the igniter, the less evidence it will leave behind. A Molotov is the easiest to keep clean, and a chemical delay mechanism leaves fewer traces than a mechanical or electrical one. Serial numbers on components can also be a problem, especially with electrical delays. In the mid-1980s, an alarm clock used in a RZ[11] action was attributed to Ingrid Strobl due to a large-scale operation by the BKA in hardware stores. Since, according to the BKA, the RZ always used the same model of alarm clock, the stock of this model was given a unique serial number and everyone who bought it was filmed. This operation resulted in two people being jailed for a long time, and the radical left movement was thoroughly investigated in

[9] *N.T.P. note:* And is therefore recovered intact by the police.

[10] *N.T.P. note:* The K.O.M.I.T.E.E. was a German far-left militant group active in 1994 and 1995.

[11] *N.T.P. note:* The Revolutionäre Zellen (RZ, *Revolutionary Cells*) were a German far-left militant group active from 1973 to 1995.

You Can Detect a Lot of What Is Being Done

An essential part of "conventional" surveillance is finding out who goes where, when, and to meet whom. But anything to do with movement is a weak point in surveillance. The surveillance operators have to move with their target while staying in contact with each other. Even if the target does not detect the surveillance themselves, there's a high probability that other people who aren't being targeted will notice it. They will see cars suddenly speeding off for no apparent reason, or people sitting in parked cars pushing themselves deep into their seats, or they will notice someone suddenly mumbling into the lapel of their jacket, or lingering in a doorway for a long time. These are all unavoidable behaviors in mobile surveillance.

So if you have reason to expect surveillance, you have a good chance of detecting it—some of it yourself if you walk around with your eyes open, some of it with the help of others.

You Are Not the Only One Who Could Be Targeted

At least in larger cities, especially in certain neighborhoods, there are hundreds of people, maybe thousands, living around the corner from you who could potentially be the target of surveillance. People are under surveillance for all kinds of crimes: receiving stolen goods, fraud, theft, robbery, murder, drugs, etc. In the political sphere, everything is possible: "terrorism", antifascists, small autonomous groups, PKK,[27] DevSol,[28] maybe even Nazis. Then there's espionage, Islamic fundamentalists, auxiliary services for foreign authorities, immigration police, searches for wanted people.

If there is surveillance in your area and you are worried that it might be targeting you, then keep in mind that there are many other people around you who might also be the target of surveillance.

[27] *N.T.P. note:* The Kurdistan Workers' Party (PKK) is a Kurdish political organization and armed guerrilla movement.

[28] *N.T.P. note:* Devrimci Sol (DevSol) is the former name of the Revolutionary People's Liberation Party/Front, a Turkish communist political party.

espionage. The elaborate, nasty technical capacities are mainly used in these domains and, of course, in the military domain.

Of course, all technically possible forms of surveillance are a potential threat to us. Anything that has been used once somewhere will be used again. The cheaper it becomes and the more familiar the authorities become with it, the more widespread its use will be.

It's also important to consider the relationship between the use of a technical capability and its success. Bugs are a good example of this: using a bug makes sense if the surveillance operators have a relatively clear idea of what is being discussed where, or at least assume that they know where interesting conversations are taking place. After all, they first have to install the thing properly and then continue to take care of it: power supply, transcription, analysis, and subsequent removal. If they assume that the target doesn't talk much or at all at home, or lives in a house with 20 rooms far apart from each other, they will think twice about doing the work that a bug requires.

When placing a camera somewhere, there are a few questions that need to be answered beforehand. Is a clear line of sight guaranteed? How good is the footage quality? If the goal is to clearly identify people, a telephoto lens must be used. This rules out the tiny camouflaged lenses, so a real camera has to be hidden nearby somehow. And a camera lens that can identify a face is also more vulnerable to being detected. If it's installed so far away that it cannot be easily detected, there's a risk that other things such as trees, cars, etc., will obscure its line of sight.

Therefore, it's realistic to assume two likely possibilities. On the one hand, there will be a handful of surveillance operations using sophisticated technical capabilities. In recent years, this has probably mainly been directed against the RAF, the RZ and Rote Zora.[26] On the other hand, the vast majority of political surveillance will use "conventional" methods, i.e. tailing the target, tapping the phone, monitoring the mail, possibly monitoring the front door with a camera.

[26] *N.T.P. note:* The Rote Zora were a German far-left feminist militant group active from 1974 to 1995.

a "§129a" case.[12]

We therefore recommend varying the selection of means and materials, such as alarm clocks. It is difficult to remove serial numbers from alarm clocks because they are often located underneath fixed components. Embossing marks in metal can be milled out, but can nonetheless be restored by the cops because an embossing die also deforms the metal underneath. Embossing marks can only be permanently removed by embossing or chiseling over them, as this changes the structure of the entire piece, just like the initial embossing process.

Fire Traces

Even though you must always be prepared for the risk of an incendiary device failing to ignite and thus leaving traces, it should be noted that even after a successful fire some traces can be analyzed. A fire leaves precise clues about what materials were used, the type of igniter and the place where the fire started. The police can reconstruct a lot from traces of soot, the gases in the air at the scene of a fire, as well as how and to what extent something was burned. Again, it is important to vary and use the simplest possible means. Always using the same mixture of accelerant or the same type of igniter is like leaving an autograph.

Writing Traces

Handwriting is very individual and easy to attribute on the basis of the lines, the dots when the pen is picked up or put down, and the amount of pressure applied to the pen. Calendars, diaries, handwritten letters and even shopping lists can be used as comparison samples. The color and ink of the writing instrument or the composition of the pencil lead can also provide clues.

Block letters are usually less identifying than cursive because many line characteristics are missing. Felt-tip and fiber-tip pens leave behind identifying writing characteristics (e.g. depending on the position of the

[12] *N.T.P. note:* The term "§129a" refers to a paragraph in the German penal code that deals with the formation a terrorist association.

hand or the pressure exerted when writing), but less so than, for example, ballpoint or fountain pens.

Remember to always write on a firm surface. Writing presses through the material underneath. If you write on a pad of paper, you will leave leave marks not only on the next sheet, but also on the following sheets. The best writing surfaces are glass or metal. Of course, nothing handwritten should be left behind or published—these handwriting tips are meant to be helpful for writing messages to each other.

Grammar, spelling, vocabulary, regional idiosyncrasies and dialect can now be compared using computer programs. This analysis is not as conclusive as handwriting analysis, but it's becoming increasingly sophisticated. The BKA has a database of extortion letters and action claims that the police use for comparison. In one blackmail case, the perpetrators tried to disguise the fact that they were native German speakers by making grammatical mistakes, but the cops were able to detect this because the authors correctly spelled difficult words.

Write simple sentences, avoiding unnecessary use of foreign words or jargon from your professional field. Vary the spelling of dates, abbreviations, and similarly distinctive references. An investigation into the alleged members of the "militante gruppe"[13] demonstrated that the police substantially cross-compare the content of action claims. Keywords and even slogans that appear in other texts—even publicly signed ones—are used by investigators to sniff in certain directions.

Proofread your texts collectively and take turns writing them. This not only prevents specialization, but also protects you because everyone has their own individual writing style. In the best case scenario, the texts cannot be directly attributed to one person. Write only the bare minimum. The shorter the text, the less material you give the cops.

[…][14]

[13] *N.T.P. note:* The militante gruppe (mg, *militant group*) was a German far-left militant group active from 2001 to 2009.

[14] *N.T.P. note:* The original PRISMA zine included several paragraphs about sending an action claim by mail, which aren't included in this translation. Today, sending an action claim through the Internet is almost always a better approach. On this topic, see the zine "How to submit an anonymous communiqué and get away with it".[a]

not by brilliant ideas or particularly dedicated working methods, but by routine, i.e. by always following the same procedures.

Another important factor is how dangerous and "surveillance aware" the target(s) is/are believed to be.

A thorough surveillance operation requires a certain amount of preparation time, sometimes several weeks. So if you've been arrested for something and you're now worried that you might be under surveillance, don't be surprised if the surveillance doesn't start until quite some time later, when your vigilance has already started to wane.

Not Everything That Can Be Done Will Be Done

There are numerous zines and books about what is technically possible in surveillance today. They describe bugs the size of a grain of dust stuck in cracks that can be accessed remotely, or camera lenses the size of a pinhead lurking somewhere. There are even cameras that no longer require lenses, using camouflaged light-sensitive micro-components instead. Tracking devices can be purchased that can be located via satellite, allowing the surveillance units to locate their target without having to leave the office. Phones can be called without ringing or otherwise alerting their owner. Rooms can be bugged from a great distance using laser beams. Computer screens can also be tapped. Thousands of phone conversations can be intercepted using computers listening for keywords.

A weakness of these texts is that they usually don't tell the reader anything about which capabilities are used when, or by whom. Many of the above techniques are very expensive. Some are technically feasible, but their development is not yet sufficiently mature and they are still in the testing phase. Others are used, but "only" by the intelligence agencies. And what the intelligence agencies have, the cops do not have—if only because the intelligence agencies value being better than the cops.

There are also priorities. Today, there are still some things that are more threatening to the State and capital than the radical left and/or that are more difficult to control with conventional methods of surveillance. These primarily include State espionage, counter-espionage and industrial

The reason for the first three forms of surveillance is usually a police investigation or something similar by the intelligence agencies and the BfV. The tightening of security laws enables the cops to surveil you even outside of an ongoing investigation.

Surveillance of an area is aimed at gaining information about the movements of various people. Against political targets, this type of surveillance operation attempts to create movement profiles for the scene. This is usually done in the run-up to important political events and may or may not be based on a specific investigation.

All forms of surveillance can also be carried out overtly. The purpose of overt surveillance is either to make the target nervous to see how they react, or to find someone to target in the first place by seeing how different people react. Overt surveillance is clearly recognizable as such. They'll show up at your doorstep or even call you to say they're there. But take note: if you detect a surveillance operation, it doesn't necessarily mean that it is overt surveillance! The operators are not always as skilled as we might assume.

It's very easy to surveil someone who is oblivious. It's very difficult to surveil someone who expects to be surveilled.

The amount of effort invested in a surveillance operation depends on many different factors. Priorities must be set: what is more or less promising at the moment? What is politically desirable, whether for the government, the local authorities, or the different factions within the security apparatus? What is even feasible?

There is competition among agencies as to who should or can do what. If one agency feels it is being interfered with in some way by another, this can lead to a reduction in the willingness to work. Although budget cuts and staff shortages impact police and intelligence agencies much less than other domains, it still does to some extent. It's also a matter of what other important cases are in progress which should not or cannot be put on the back burner.

The surveillance apparatus is a sluggish public service system with a lot of people who don't really care about their job. Success is often achieved

It's becoming more popular to use a Linux computer with a "live system" that runs in memory. But we should briefly discuss problems with printing. Printers leave traces, so your home printer is not suitable for anything sensitive. At least color laser printers are known to hide their serial number in the printed sheet.[15] We do not know if this problem also applies to copiers, but it should be assumed. Keep this in mind when printing anything! The same problem exists with CD and DVD burners. They burn the unique serial number of the device onto the CD.

Material Traces

By material traces (also known as "trace evidence"), we mean all traces that are unintentionally left behind on you, on your clothes or in places you have used. Again, there is no such thing as 100% security, but we can at least make the cops' job more difficult.

Let's start with traces on your clothes. Though invisible to the naked eye, there are many traces on your clothes that can't necessarily be removed by washing them. Depending on the type of action, these traces can be used by the cops in different ways. If you use spray paint, you can be sure that even though you can't see it, fine particles of paint will be on your clothes, especially on your pants and shoes. The police can make these particles glow with a special lamp which is available in every police station. These traces of paint cannot be removed.

It's also impossible to remove the fine glass particles that are created when a pane of glass is broken. Unfortunately, these particles can be attributed to a specific pane based on the type of breakage. Again, washing clothes is of little help. Blood stains are also impossible to remove.

Disposing of your action clothing is often the only way to be as free of traces as possible. A simple, inexpensive coverall from the hardware store can help. You can take it off soon after the action and wear inconspicuous clothing underneath. However, be sure to practice taking it off beforehand

---

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

[15] *N.T.P. note:* For more information on how printers hide information in printed sheets, see "Printer Tracking: Is Your Printer Spying On You?".[a]

[a] https://notrace.how/resources/#printer-tracking

and, if necessary, cut the bottom of the pant legs a little so you can get it over your shoes. Under no circumstances should you dispose of it near the action site, as it is sure to contain at least some traces of your DNA. We have already covered the topic of shoes and shoeprints.

Any clothing you wear will leave traces on your body. This is especially important if you are wearing gloves, as the cops will be able to tell that you were wearing gloves, and which ones, by looking for traces of fibers under your fingernails, for example. Disguises such as beards and wigs also leave traces. Although it's almost impossible to prevent this, you should be aware that even after changing clothes and putting some distance between yourself and the action site, you will not be completely free of traces, and you may have left traces of fabric behind.

It is important to not wear anything with buttons that could get lost, and to avoid long scarves or clothing with fringes. Not only will they hinder your escape, but fabric can easily be left behind at the action site.

If you come into contact with gasoline during the action or while building a device, you should be aware that the scent is almost impossible to remove, which may be a problem if you are stopped by the police. Be careful not to spill accelerant on your skin or clothing when throwing a Molotov. The problem here is your own sense of smell—your nose develops a certain tolerance to a smell after being exposed to it for a long time, and you will no longer be able to tell if you smell like a small gas station.

If this is the case, and for example if they are investigating an arson, the police may put your hands in plastic bags so that they can later analyze whatever traces were on them. This is especially true for traces of gunshot residue that are left after firing a gun. Smoke residue tests are now also used to determine if an arrested demonstrator shot a firework or if someone set fire to a car with firelighter cubes. Traces of smoke often remain even after washing, which is another reason to dispose of your gloves.

Making action materials can also leave traces. If you work with powdered substances, you must assume that both your workspace and your clothes will be full of them. As far as we know, it's impossible to completely clean

in very few exceptional cases. And hardly anyone will think about life jackets throughout the entire flight.

When we talk about surveillance in this text, we mean the targeted surveillance of specific individuals. We will not go into detail about the everyday snooping that affects a scene in general, such as collecting scene publications and posters or hanging around in the relevant bars and public meetings.

First, a Few Basic Rules When It Comes to Physical Surveillance

A surveillance operation is planned and organized. It requires some effort if it is to be useful: preparation, personnel, vehicles, technical aids, coordination. Most surveillance has no political motivation and is carried out against threats such as organized crime, burglaries, etc.

There are various forms of surveillance. They can be categorized as follows (the terms are chosen by us): surveillance of a specific place, object, person, or area.

In the case of surveillance of a place, the surveillance operators sit in a static location (in a house, car, etc.) and do not move from there. For example, they may be exclusively interested in who enters a certain building, or whether something is hidden in the bushes somewhere. Such surveillance is very difficult or even impossible to detect.

Surveillance of an object is a variation of the first form. It involves keeping an eye on a specific object, such as a car or a parcel of money. To do this, the surveillance operators have to be mobile.

In the case of surveillance of a person, the first two forms can be combined. For example, by monitoring the target's home with cameras (static surveillance), and otherwise tailing the target (mobile surveillance). In some cases, tracking devices may be used, or the operators may set up at fixed locations that a target must pass. Surveillance may end in an arrest, or it may have no noticeable consequences at all, except that the security authorities hold onto everything they have recorded.

All of us who are close to anti-authoritarian ideas (and hopefully actions) are familiar with this time of year. Many of us have experienced various forms of repression in our years of political activity: the police baton at demonstrations, investigations, trials, raids, prison. Although these directly experienced patterns and forms of repression can be somewhat demystified over the years, it is always frightening how little we collectively learn from these experiences. New campaigns for refusing to testify in police stations and during trial continue to be necessary, and people still feel helpless when caught in the thorns of the court and prison apparatus, often repeating the same old mistakes. There are piles of texts on all kinds of repression, but it makes a big difference whether you experience something yourself or just read about it.

What is true of direct, overt experiences of repression is all the more true of the more covert forms. The radical left knows a lot about the apparatuses of its enemies, or at least has theoretical knowledge, but in practice takes them into account rather sloppily.

The subjective feeling of being threatened often determines one's actions: “Nothing will happen”—“What could they possibly want”—“I'll be careful”—“After all, they don't have my fingerprints yet”—“Why would they be interested in me?” But also: “I'm surrounded”—“Nothing works anymore”—“It's better if I stop being active”—“Everything is surveilled anyway”—“Orwell's '1984' has been surpassed long ago.”

On the other hand, some people apply general principles to avoid needing to precisely evaluate a particular situation: never talk in your own home, especially not over the phone, keep no written documents, etc.

This text is intended to shed some light on the shadows of surveillance. It has two main objectives. Firstly, learning and knowing the methods of the enemy means being able to fight them! Secondly, down with paranoia!

We are aware that dealing with this topic in detail may stir up feelings of paranoia. Those reading this text should keep in mind that everything described here is an exceptional situation, perhaps comparable to airplane travel: before takeoff, instructions are given on the use of life jackets, and everyone should be familiar with how to use them, but they are only used

a workspace such that nothing is found by chemical forensic methods. So if you want to be on the safe side, your home should not be used for this type of work. Instead, use places which seem safe and cannot be traced back to you (i.e. not places linked to the radical left!), such as abandoned buildings. Wherever you end up working, you should be careful to avoid leaving behind any fingerprints, DNA traces, or pieces of wire, no matter how small.

Purchases

You should be especially careful when shopping. Buy only one item at a time in a store. Pay with cash, not a credit or debit card. Destroy your receipts. Think carefully beforehand about what you are going to buy and where, and perhaps test the store with something inconspicuous to feel it out.

Large stores with lots of customers allow for some anonymity, but usually have surveillance cameras. Sometimes the footage is deleted after 48 hours. Take advantage of this and plan ahead, but don't rely on it. It's always better to shop a reasonable amount of time before an action. This way, you won't be in a hurry and get careless if something isn't available. Small stores have the advantage that they often don't have surveillance cameras, but cashiers can be very good at remembering who they sold what and when.

Small disguises can go a long way to make you unrecognizable. From non-prescription glasses to fake beards, wigs, colored contact lenses and hair dyes, from suits to jogging outfits, there are no limits to the imagination. Even theatrical makeup or latex masks can be useful. However, you should feel comfortable in your disguise and appear normal and inconspicuous.

If possible, always buy everything in packaging. Ask for a bag, the cashier will often pack your purchases for you. In winter, it can be inconspicuous to shop with (unused!) gloves. If gloves are too conspicuous you can use liquid bandage to somewhat reduce fingerprints (see Fingerprints, p. 6), but this doesn't completely prevent them, and you will still leave DNA traces.

Do not go shopping with your car or motorcycle. Of course, you should also leave your mobile phone at home. The same precautions apply when shopping as when doing reconnaissance at the action site. If you do actions frequently, vary which stores and brands you use, as well as the time periods and days of the week you buy certain items. Sometimes it's worth traveling a bit further away or even to the next town. Make sure it isn't possible to determine where you live based on your purchases.

For specialty parts, come up with a story that explains why you need them for legal reasons. Do your research beforehand. Also prepare a story for small talk with other shoppers, just in case. Some chemicals require your signature. Practice a fake signature and use block letters for forms. Bring a felt-tip pen (see Writing Traces, p. 18).

A Few Research Tips

When you prepare for an action, you leave behind not only material traces, but digital ones as well. Here are a few basic procedures for doing research in preparation for an action.[16]

The books you order or borrow from a library can be traced back to you, and the cops check the library accounts of suspects. Avoid libraries at all costs. Some libraries are also under video surveillance. […] Leave your mobile phone at home when doing research.

Remember that Internet cafes often have surveillance cameras, so try to avoid them. […] You should be aware that even in cafes without cameras,

[16] *N.T.P. note:* In the original PRISMA zine, this section assumed that you would do research for an action using a public computer at an Internet cafe or a similar location. We advise against this, and therefore omitted most of the original section in this translation. From "How to submit an anonymous communiqué and get away with it":[a]

> "The general recommendation for most people is to use a personal computer that is only for Tails, on public WiFi. […] Public computers themselves could be compromised at the hardware level or through intentional collaboration between their owner-operators and law enforcement, and this could be almost impossible to detect."

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

will also help if you are well masked or not positioned in the camera's field of view. Though it's easy to make mistakes in this regard as some cameras have a wider range than is apparent from the outside. Sometimes it's enough to wear clothing that conceals your body shape, such as a garbage bag, or to put a rain cover over your bike to obscure it (when the camera is far away). Afterwards, you should dispose of your clothes and, of course, not use your everyday clothes in which you may have already been photographed. We recommend reversible jackets, masks, umbrellas, or placing cushions and pillows under your clothes that change the shape of your body. Beards, wigs, paint on your face, or pieces of apple in your cheeks can also change your face. However, always consider whether the circumstances allow you to be a little sloppy with the (possible) cameras! If in doubt, don't do it, rather than put yourself at unnecessary risk!

Physical Surveillance

> Originally published as Tausend Augen (*A Thousand Eyes*) in part 2 of issue 153 of the German magazine *radikal*. The comment in square brackets is from the editors of the original PRISMA zine.

[This text is a bit old, but still quite relevant. It will be clear to anyone who has walked down a busy street that mobile phone technology has evolved…]

Eyes stare out of windows everywhere you go… A car rolls slowly past you, two young guys sitting in it, watching you out of the corner of their eyes… Another car has been parked in front of your door for days… The phone suddenly crackles in a way it didn't before… A satellite antenna has recently been installed on the house across the street, pointing directly at you… A helicopter has been flying over your street a lot lately… Someone has asked for you… Beyond the blue summer sky, a spy satellite orbits and photographs you fifty times per second as you walk through deserted streets…

The season is called PARANOIA.

record in different ways depending on the application. As a deterrent, sometimes only fake cameras or "You are being recorded" signs are installed without a device actually being present. If the recordings are meant to be used to investigate possible crimes, they are not only displayed on monitors but also saved. Saved recordings can later be viewed remotely or accessed via the Internet. All of these variants can be wireless or wired.

In terms of camera types, there are large, highly visible cameras that are preferred for deterrence. These are the traditional box cameras, box-shaped long-range infrared cameras or the large versions of dome cameras. Small to medium-sized pen cameras (round, pen-shaped), small dome cameras or mini cameras are used as recognizable but more inconspicuous, discreet cameras. And, of course, there are hidden cameras: very small mini cameras (e.g. integrated almost unnoticeably in doorbells, on front doors or gates), and cameras that are completely disguised in clocks, behind one-way windows, in motion detectors or smoke detectors.

All camera types can be equipped with various functions: zoom, pan and rotate, extra wide radius, night vision. They vary in their sensitivity to light, type of focus (variable or fixed), and image resolution. With high resolutions, people or license plates can be recognized and identified. So-called "intelligent cameras," which recognize previously stored characteristics of people, such as eye-mouth-nose distance, iris or gait, and then sound an alarm, are not yet in use in Germany. In general, the latest technology is not used everywhere, but it tends to get better and cheaper. The type of camera and its capabilities cannot be identified at street level, or only roughly. So your assessment of a camera type can be based on the location and the level of surveillance you think is likely there.

What Can We Do About Them?

We can choose our routes and targets so that no surveillance cameras record us. But we can also try to outwit them: hold something in front of the camera if it isn't mounted too high (e.g. an umbrella, cardboard, or even just a bag placed over the lens). Spray paint the lens or apply paint with paint sprayers or eggs filled with paint, apply stickers or cut the cables (be careful, always use insulated tools!). Stones or hammer blows

staff may still be able to remember you. Try to wear disguises and be as inconspicuous as possible. Remember that your fingerprints can also be found on cash you handled, at least for a short time.

Technical Surveillance

> Originally published in Repression und Widerstand (*Repression and Resistance*). With small additions from the editors of the original PRISMA zine.

What technical capacities are used for surveillance? And how can we counter them?

We've all seen it in spy movies: bugs in lamps and cameras behind one-way mirrors in 1960s thrillers. Or the modern operations centers in more recent movies that can listen in on every phone call within seconds and track everyone via satellite surveillance.

The reality is somewhere between these two portrayals. Not every police force has access to the same technical equipment (and trained personnel), and will only request it if the associated costs can be justified with an appropriate threat scenario or serious "crime" that has already been committed.

Nevertheless, the State's interest in prosecution and criminalization should not be underestimated. Police and intelligence agencies will try to justify the purchase and maintenance of expensive equipment by using it as frequently as possible.

This text explains the current technical capacities of police and intelligence agencies (as of 2006). The most effective countermeasures are very simple and can be implemented without detailed technical knowledge: meet in places where surveillance is highly unlikely and do not use risky communication channels (phone, mail) for political purposes.

Monitoring Enclosed Spaces

All of the instruments available for monitoring enclosed spaces have two major disadvantages: they require advance preparation and they are relatively expensive.

Bugs

Of all the listening methods described here, bugs provide the best sound quality. Depending on what they are used for, they can be very small (2–3 millimeters thick), but can also be the size of a sugar cube or even a matchbox. They are almost indistinguishable from other electronic components and are sometimes camouflaged, i.e. permanently installed in other objects, rooms or vehicles.

Preferred places to install bugs are electrical outlets, light switches, landline phones and other electrical devices that are continuously supplied with power. If necessary, holes are drilled in furniture to place microphones as close as possible to the people speaking.

Bugs can eavesdrop on conversations within a radius of about 10 meters. One bug is enough to monitor a room of about 100 square meters. Depending on its battery, a bug can operate between several weeks (button cell) and several months (9 volt battery). Of course, bugs that are connected to an electrical source or a phone cable will "live" longer.

Bugs with built-in radio transmitters are among the larger variants and can reach radio ranges of several hundred meters or up to two kilometers, depending on the building.[17] Electrical and phone lines can also be used to transmit the intercepted conversations.

Special microphones hidden in landline phones or their jacks can be remotely activated and listened to.

Countermeasures against bugs:

[17] *N.T.P. note:* As of 2025, it appears that the majority of bugs used by police and intelligence agencies that remotely transmit their recordings do so through the mobile phone network. Those bugs can transmit their recordings as long as they can communicate with a cell tower.

number has increased in recent years and will continue to do so. However, we shouldn't let this deter us from doing what needs to be done, but rather we should increase our knowledge—about their proliferation, their technical capabilities, and how we can render them harmless.

Where Can You Find Them?

(Almost) always in places considered sensitive to the State, such as banks, embassies, ministries, warehouses, the homes of high-ranking individuals, and corporate headquarters. Often and increasingly at train stations, on trains and buses, in front of garages, driveways, parking lots, and store entrances, where they sometimes also record the sidewalks. Internet cafes and sometimes even copy shops are often monitored by cameras. Targeted camera surveillance of public places is still very controversial and therefore exists only in isolated cases and with media attention. Entrances to well-known places of the radical left, autonomous social centers or squats are monitored as inconspicuously as possible and usually not continuously, if they are monitored at all. However, individual cases of continuous camera surveillance over many years have been revealed during political trials. It's certainly worth observing the windows opposite the entrances of such places (even at a very oblique angle). The BfV sometimes rents apartments for this purpose. Normal tenants have also been asked to make their windows available for a surveillance camera. A secondary entrance and exit, via courtyards or rooftops, may therefore be useful. Of course, cameras can be installed there as well.

Recordings made with mobile phones are increasingly becoming another source of danger. They can be used to film or photograph people in locations that are far away from any buildings. We also shouldn't forget the police who are constantly recording at demonstrations. Journalist footage or private recordings can also be seized by the police.

What Can They Do and How Can They Be Recognized?

Several books could be filled with information on camera types and applications, but a rough overview will suffice here. Surveillance cameras

E-passport

Following an EU decision, since November 2007 German passports contain biometric data. As of November 2007, this involves two fingerprints. This data (as well as most other passport data) is stored encrypted on a newly introduced RFID chip. You can find out what data is stored from the passport authorities.

The new passport is touted as being extremely forgery-proof. As with all RFID chips, there is a risk of unnoticed reading. To prevent this, the chip only transmits after the "standard" passport data have been read. The reader tells the chip that it knows this data, and the chip then makes itself readable.

Doesn't sound bad at first, at least if you trust the technology created by the State and its compliance with the law. If this trust is lacking, you can shield the chip (with aluminum foil or a protective cover that can be purchased). In principle, the chip can also be destroyed, e.g. in a microwave: Put the passport in, set the microwave at its lowest level, and switch it on very briefly (shorter than briefly). The passport remains valid even if the chip is not working (but only the chip—burned holes in the cover are bad, of course).

Surveillance Cameras

Imagine: the cops end up arresting Anna[25] near a smashed police station. Anna is found not guilty because she was wearing a mask (of course!).

For our own security, when we do reconnaissance, carry out a clandestine action, and leave the action site, we must make sure that no surveillance cameras are recording us. Sometimes they are very small and hidden, sometimes they are large and obvious or installed as a deterrent. The latter is unfortunately not always the case, especially when police and intelligence agencies have installed them for surveillance purposes. Their

[25] *N.T.P. note:* The name "Anna" is a reference to a slogan of the German radical left encouraging people to not give statements to the police, "Anna und Arthur haltens Maul" (*Anna and Arthur keep their mouths shut*).

Of course, anyone can search for bugs themselves. Special bug detectors are available for purchase at different price ranges, and services can also be hired. Professional bug hunters charge a lot of money. And they usually have a history as intelligence agents, military personnel, or police officers, and will therefore be wary of fouling their nests.

If you find bugs, it's proof that a bugging operation took place, but there's no guarantee that there aren't more hidden microphones which haven't been found.

Playing music, tapes of other conversations, or the radio does not help prevent bugging. Modern technology can easily filter out individual voices.

Special audio jammers can help. The noise they produce is barely audible to the human ear, but prevents the recording of conversations. They also help against the other eavesdropping capabilities described below and are available from around 500 euros.

If you really want to be on the safe side, you should generally refrain from mentioning important dates, places and actions and instead use pen and paper and then destroy what you've written.

[…]

Stethoscopes

Rooms can be listened to from the outside using electronic stethoscopes.[18] These devices can amplify the smallest sound waves that pass through walls, doors, and water pipes up to 40,000 times to make them audible. This can be prevented by audio jammers equipped with special contact resonators.

Window Panes Vibrations

The noise generated in a room causes the window panes to vibrate slightly. Using an invisible infrared laser, these vibrations can be measured at a distance of up to 200 meters and converted back into sound waves. Complete systems (transmitters and receivers disguised as cameras,

[18] *N.T.P. note:* Contact microphones[a] can also be used for the same purpose.
[a] https://en.wikipedia.org/wiki/Contact_microphone

amplifiers, and noise filters) are available for less than 10,000 euros and are therefore likely to be used relatively frequently.

The drawbacks of this technology are that there must be a line of sight to a window in the room being monitored, and that the results are rather poor for double-pane windows.

Video Surveillance

Cameras with built-in radio transmitters can be as small as a matchbox. And the lenses of such cameras are barely larger than pinheads and can be camouflaged very effectively. For example, they can be hidden behind stickers or disguised as Phillips-head screws. Completely camouflaged systems are also available in the form of smoke detectors, desk lamps, and other everyday objects.

These special cameras can capture footage of very high quality. Their operating time and radio range are comparable to those of acoustic bugs. Cameras can be found with bug detectors if they are equipped with radio transmitters.

Phone Surveillance

In 2004, more than 30,000 phone surveillance orders were issued in Germany to investigate criminal offenses. In more than 60 percent of the cases, the conversations of uninvolved people were tapped, while the conversations of suspects accounted for just under 40 percent. These figures do not include wiretaps by intelligence agencies or preventive police measures.

Internationally, Germany is considered the world champion in wiretapping, and the numbers are increasing every year. In December 2005, the new federal government announced that it would revise the related legal regulations by mid-2007 (under pressure from the Federal Constitutional Court).

According to the law, anyone whose phone has been tapped must be informed after the investigation is completed, but this rarely happens.

characteristics used include an individual's body size, iris and retina, fingerprints, facial geometry, handwriting, DNA, voice, gait, or even typing behavior on keyboards.

Most of these methods are still in the testing phase; their results are either too inaccurate or too complicated to use in practice. Currently, iris, retina, fingerprint, and facial recognition systems are the most common. There are currently very few such systems in the public sector. Examples include the Hannover zoo, where visitors with an annual pass are admitted using a facial recognition system, or the Frankfurt airport, where travelers can pass through border control with an iris scan (in conjunction with their passport).

Facial recognition systems measure the relative distances between the eyes, nose and mouth, usually starting from the eyes. To be correctly identified, a person must be facing forward, still, and very close to a camera (and their face must have been previously filmed or photographed from the front, measured, and then stored in the relevant system). There are already attempts at 3D recognition, i.e. the ability to recognize faces from any angle, but these are not yet ready for practical use.[23]

In addition to access control, the automatic identification of wanted persons with the help of publicly installed surveillance cameras is an aspirational and advertised goal.

All attempts to do so have failed due to the high frequency of false positives. It's not possible to estimate how long it will take before these systems can automatically identify wanted suspects in real time. It's also possible, for example, to manually "cut out" faces from photos of demonstrations and have them identified automatically.

A relatively simple trick to prevent this (or unwanted facial recognition in general) is to wear sunglasses or a low-cut baseball cap.[24]

---

[23] *N.T.P. note:* As of 2025, facial recognition systems can recognize faces from different angles.

[24] *N.T.P. note:* As of 2025, wearing sunglasses or a low-cut baseball cap does not necessarily prevent facial recognition. On this topic, see the text "How To Prevent Facial Recognition Technology From Identifying You".[a]

[a] https://notrace.how/resources/#prevent-facial-recognition

- Bank and credit card accounts: They provide information about money movements. Using debit and credit cards also generates information about transactions, including their exact time and place.
- Libraries and mail-order bookstores: This can reveal the political interests of individuals and is therefore highly relevant to mass surveillance. Amazon has already been forced by U.S. authorities to hand over its user data.
- Of similar importance are the semi-legal file-sharing networks that allow downloading movies and music. The only difference here is that users of those networks usually do not leave any personal information other than their IP address.
- Membership lists of political and religious communities, and martial arts schools and clubs.
- Air and rail travel: The names of all passengers on flights to the U.S. are submitted to U.S. authorities. Depending on the potential threat posed by such passengers, several airplanes have been forced to turn back or land in Canada. Depending on the "threat situation" and the government, such surveillance can also be implemented in Germany and other European countries.

Security countermeasures are not straightforward when it comes to data collection. Of course, we all have bank accounts and need to withdraw money from ATMs from time to time. But if you don't want to leave too much of a trail, you should be extremely careful about giving out personal information and as much as possible avoid ordering things online or paying by card. Cash payments leave the fewest traces.

Biometrics

Biometrics is a branch of science concerned with the collection and analysis of physical and behavioral characteristics of living beings. When applied to humans, the focus is on computer-aided identification ("Who is this person?") and authentication ("Is this person who they say they are?"). In practice, this is intended to prevent unauthorized persons from gaining access to rooms or systems to which they shouldn't have access, even if they have stolen or otherwise acquired PINs or passwords. The

The high rate of cases of phone surveillance comes from the fact that it is one of the easiest surveillance measures to carry out—they simply obtain a court order and notify the relevant phone company. All calls to the targeted phones are then redirected to another number or voicemail for monitoring. Because all the equipment used is digital, there is no telltale crackling or hissing.

The phone companies do not record calls without a court order. However, all call metadata is recorded—the exact details of when and for how long the call was made and to which number. This metadata can be crucial to police investigating crimes that have already been committed. For example, it can provide a basis for identifying social connections in a scene, or help prove the existence of an alleged criminal association.

The BfV[19] and foreign intelligence agencies are constantly listening to as many phone lines as possible for telltale keywords. This surveillance is fully automated with the help of sophisticated voice recognition software. This software is capable of linking information together to create patterns of meaning. Conspicuous conversations are stored and then manually analyzed. It is highly likely that voice recognition will also make it possible to identify somebody with a recording of their voice.

All international calls are intercepted. Intelligence agencies will almost certainly intercept all satellite calls.

The most advanced interception system of this kind is operated by the English-speaking intelligence agencies under the name "Echelon". The US National Security Agency (NSA) alone employs about 28,000 people for this purpose and is able to record and analyze a large portion of Internet communications.

There is relatively close cooperation between intelligence agencies, especially when laws make it difficult to surveil one's own country.

[19] *N.T.P. note:* The Bundesamt für Verfassungsschutz (BfV, *Federal Office for the Protection of the Constitution*) is Germany's federal domestic intelligence agency.

Landline Phones and Fax Machines

Landline phones can also be tapped directly without the help of phone companies. Bugs in the phone, in the wall socket, in the house switch box or in the distribution box on the street are relatively easy to install.

Fax connections are intercepted in the same way. "Dumb" phones make their job even easier—their signals can be intercepted and decoded from just outside the home.

Public Payphones and Phone Cards

It's also possible to monitor all phone calls made with a phone card from public payphones. To do this, the cops make the operator transmit all connection data for this specific phone card number.

Mobile phones

Mobile phones can be tapped with the help of phone companies. And they offer additional attack vectors for investigators: they can be used to determine the user's location, their communications can be intercepted by IMSI-catchers, and they can be infected with malware.

[…][20]

Countermeasures

There is not much that can be done to prevent landline and mobile phone calls from being tapped.[21] At best, it would be possible to use coded language when making calls. But it's safer to avoid phone communications altogether when dealing with sensitive content, i.e. to avoid scheduling meetings and demonstrations by phone.

[20] *N.T.P. note:* The original PRISMA zine included a longer section on mobile phones, which isn't included in this translation because it contained errors and inaccuracies. For more information about mobile phones, see AnarSec's guide "Kill the cop in your pocket".[a]

[a] https://anarsec.guide/posts/nophones

[21] *N.T.P. note:* To prevent phone communications from being tapped, you can use smartphones with end-to-end encrypted messaging applications. For more information, see AnarSec's guide "Encrypted Messaging for Anarchists".[a]

[a] https://anarsec.guide/posts/e2ee

The main problem with RFID chips is that the owner has no control over what information is requested and retrieved via these chips, when, and by which "reader."

Depending on the design of the chips, the police could determine a person's identity by radio at any time without them noticing or being able to prevent it. It would be possible to see which debit card they have and that they have just purchased certain products (or are carrying products that are not marked as "paid for"). Horror scenarios such as "scanning" entire demonstrations or "sensitive" locations are also conceivable.

Fortunately, there are simple and effective countermeasures against this type of spying: RFID chips wrapped in aluminum foil completely stop working. Separating the millimeter-sized chips from their larger antennas also renders them useless.

Databases

Virtually all companies want to collect as much data as possible about their customers. Customers have only limited control over this collection, and even when very strict legal regulations exist, in practice they are not enforced. And the data protection regulations can be overridden by a customer signature.

These databases don't just store data on all transactions (purchases, orders), complaints, information requests, etc. With the help of appropriate software, reasonably accurate customer profiles are also created, by "residential area", "number of phone connections per house" and similar publicly available data. The next time someone calls a company, this can determine whether they are put through immediately or put on hold.

In addition, various "data brokers" offer data for sale that they could not have obtained legally.

Even if very few of these corporate data collections are directly "tapped" by surveillance authorities, they can be stolen by hackers, for example, and possibly end up with the police as part of an investigation.

Typically, police and intelligence agencies have a much greater interest in the following types of customer data:

black-and-white cameras are used, but black-and-white cameras are more sensitive to light and can be easily combined with infrared systems.

There are two trends in video surveillance:

- Automatic License Plate Recognition works virtually flawlessly and is already used in truck tolling systems. These systems also record the license plates of cars that are not subject to tolls. Both the license plate and the driver are photographed. So if it's not possible to avoid toll cameras, you should make sure that at least the passengers are not recognizable in the photos. For example, you can fold down the sun visors and tilt them to obstruct the view from the cameras.
- Several major German cities plan to go much further. They want to setup systems that specifically search for wanted license plates. Hamburg has already adapted its police law to use mobile surveillance cameras for this purpose.

RFID Chips

Radio Frequency IDentification (RFID) chips are used in applications like car keys, library books, tickets for the World Cup, and to track animals. The integration of these chips into credit cards and new passports is concerning. Another application being discussed is car license plates with RFID chips.

In supermarkets, RFID chips are intended to eventually replace today's barcode price tags. At the checkout, all items will be automatically identified by radio. The RFID chips are then marked as "paid" but can still be read.

To read RFID chips, a "reader" interacts with them wirelessly via radio waves, and the chips send back the requested data. RFID chips can be rewritten several times with different data.

The commonly used "passive" RFID chips do not require their own power supply. They draw their power from the radio waves they receive and are connected to long, usually helical antennas. The range of most of these chips is from a few centimeters to several meters.

It's best not to bring a mobile phone to demonstrations and other political events. If you still need a phone, it's best to get a second device with an empty contact list, call log, and SIM card, used only in such "insecure" situations.

Mobile phones should be left at home before anyone leaves for a meeting or event. Especially if it takes place in a location you don't normally frequent.

By the way, caller ID suppression is ineffective when the police are involved.

Postal Service

Letters can be scanned with X-rays, which makes it easier for the snoopers to decide whether the mail is worth opening. Wrapping the mail contents in aluminum foil prevents effective scanning, which probably makes the package really eye-catching. Letters can also be opened with steam.

Vehicles

The Global Positioning System (GPS) makes it possible to determine a position with a precision of a few meters. The system has been operated by the U.S. military since the early 1990s and currently consists of 28 satellites, 4 of which are accessible at any given time. In 2000, the artificial inaccuracy introduced for civilian GPS devices was removed. Since then, GPS has been used in applications like car navigation systems, and by police and intelligence agencies for monitoring vehicles.

GPS trackers can be smaller than a matchbox and determine their position about every 10 seconds. Depending on the model, this data is stored locally or sent by radio (usually through the mobile phone network) to the monitoring agency where it can be displayed over city maps.

GPS trackers can be easily attached to the underside of cars using magnets or glue. In rare cases, they can be noticed by a buzzing or humming sound when the car radio is turned on.

In addition to GPS trackers, smaller radio trackers (15 x 35 mm with a 15 cm antenna) are also used, and require significantly less power. Thanks to their small size, these transmitters can be installed in bicycles and smaller portable objects. However, they do not transmit position data. A receiver can only determine the direction the signal is coming from. This makes it easier to tail someone, for example.

Of course, all bugs that can be used in buildings can also be used in vehicles. Preferred locations for the installation of such devices are the interior side panels and the roof of the car. The lights built into the roof can provide a power supply.

In Germany, there are growing calls for the mandatory installation of so-called accident data recorders (ADR). These "black boxes" store all important data, especially speeds and distances, which are intended to be used to reconstruct accidents, but are of particular value to the police during investigations. They are standard in U.S. cars. In Europe they are used in rental cars and in some car models.

Public Space

With the help of modern surveillance technology, police and intelligence agencies are often closer to what is happening in public than their targets would like them to be. Binoculars, night vision devices, and directional microphones can be used to listen to, photograph and film conversations from a significant distance. Therefore, outdoor meetings should be planned and conducted with at least as much care as indoor meetings.

Directional Microphones

Small and handy, they can pick up conversations from 50 to 200 meters away, depending on the model and the line of sight. They amplify only the frequency range of the human voice and can therefore also be used in noisy environments such as pubs.

It's not possible to listen into closed rooms (through windows or walls) with directional microphones (although this is possible with other tools such as stethoscopes).

Binoculars

Portable binoculars can clearly identify faces up to a distance of about one kilometer. Cameras attached to these binoculars can be used to take photos and videos.

Night Vision Devices

Residual light amplifiers make it possible to see in partial darkness by amplifying the existing weak light.

"True" night vision devices work in total darkness by illuminating the surrounding environment with infrared radiation. This light is invisible to the human eye. The night vision device displays it in black and white. Since infrared radiation penetrates fog better than light, these devices can be used in poor weather conditions. More advanced night vision devices use millimeter wave radiation instead of infrared radiation and can therefore also see through thin walls.

Thermal imaging devices operate without the need for residual light or an artificial source of infrared radiation. They graphically display the heat given off by the objects they observe and are used, for example, to check the insulation of houses. During the Castor rail blockades,[22] these cameras were used from the air to locate people hidden in open areas and forests. They can also be used to detect recent changes to the ground. However, heavy rain, fog, or blowing snow can limit their effectiveness.

Fixed Surveillance Cameras

An increasingly dense network of fixed surveillance cameras is being installed in Germany, with the aim of increasing security in streets, squares, and public transport. In train stations and airports in particular, almost every square meter is covered by video surveillance. The number of cameras installed in subways and buses is also growing.

The footage from surveillance cameras is usually displayed live on monitors (e.g. in control centers) and also stored for later review. Both color and

[22] *N.T.P. note:* From the mid-1990s onwards, many anti-nuclear protests in Germany, including rail blockades, were directed against transports of radioactive waste called "Castor".