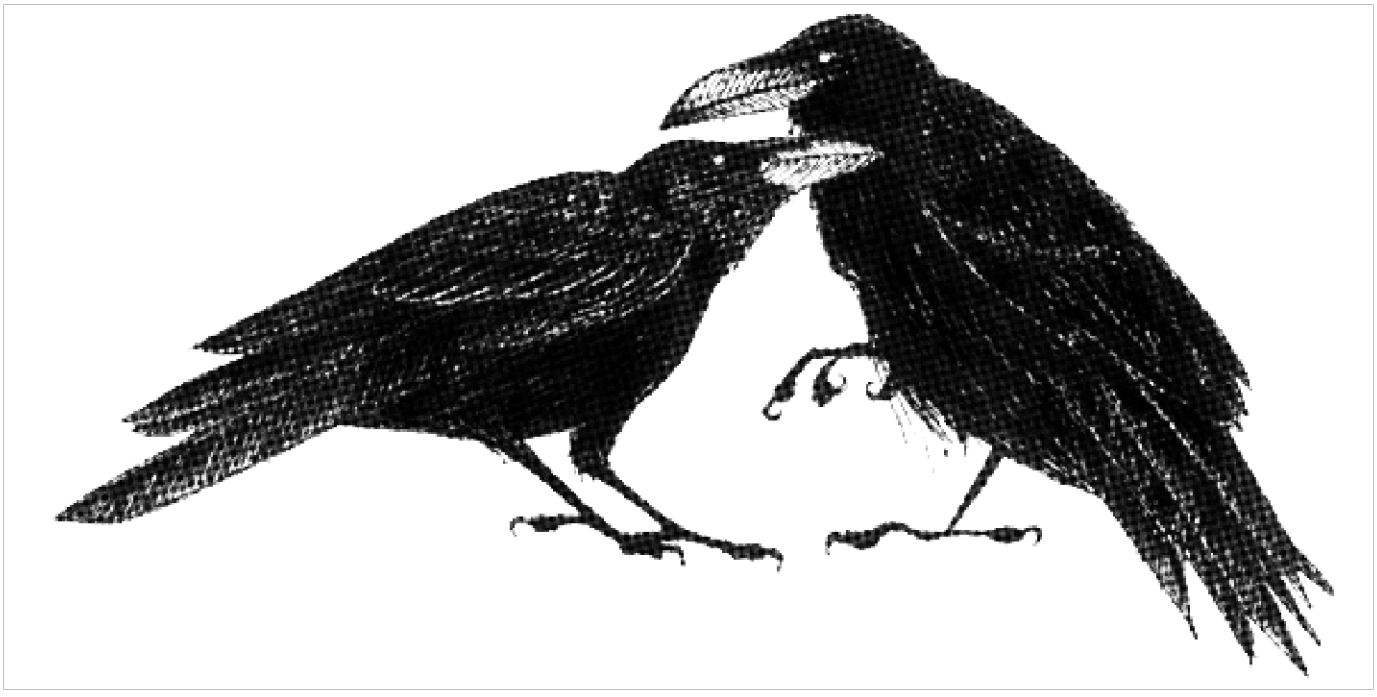
Establishing a Security Baseline for Anarchists and Radicals



Establishing a Security Baseline for Anarchists and Radicals

Original text in English
Tinderbox: An Offline Journal of Combative Anarchy, #8
2025

Layout
No Trace Project
notrace.how/resources/#establishing-baseline

The Tinderbox collective gave permission for this article to be published online.

This text was written in response to an ongoing need in Philly and elsewhere for tighter security practices. It also responds in part to the No Trace Project's "To the International Anarchist Movement: Three Security Proposals",[1] which includes a proposal to establish security baselines locally. The authors write:

> "Anarchists who carry out direct actions should analyze the risks associated with their actions and take appropriate precautions: dress anonymously, be mindful of video surveillance and DNA traces, and so on. However, this is not enough. If only those who carry out actions take precautions, it is easier for our enemies to target these individuals. This is, firstly, because they stand out: if only a handful of comrades always leave their phones at home, for example, this could be an obvious starting point for an investigation with no other specific leads. And secondly, because our enemies can get information about them through their friends who do not carry out actions: if someone doesn't use social media but is mentioned on their friends' social media, for example, an investigation could query their friends' social media to get information about them. We should therefore establish a security baseline that everyone in anarchist networks agrees to follow, including those who have never carried out direct actions and have no intention of doing so."
>
> "It can be difficult to convince people to follow such a security baseline, especially if they think they have no personal interest in following it. If someone is reluctant, we should remind them that it's not just their security that's at stake, but also the security of other anarchists around them who may be carrying out or planning to carry out direct actions. Everyone who wants actions to happen has an interest in making anarchist networks as difficult as possible for the authorities to repress."

[1] https://notrace.how/blog/three-proposals/three-proposals.html

In this text, we try to identify specific needs, for example for various kinds of communication with each another, and establish some baseline practices around meeting those needs that we can all share to make ourselves harder targets for state repression. We feel that this is especially urgent in this era of increased repression of many oppressed populations in the U.S. and of resistance more generally. This repression has been unpredictable, chaotic, and terrifying. We can empower ourselves to keep fighting for anarchy and liberation by establishing some shared practices in the Philadelphia anarchist/radical space that make us all safer.

That being said, the state's response to strong radical struggles is never gonna be pretty or predictable, and we would offer similar recommendations about security practices regardless of who is running the country. These recommendations are based in part on the current level of radical activity that's going on in Philly, but they're also tailored to the level of activity that we're working towards, to what we see as our potential. This might include the return of widespread prolonged uprisings in the streets. Or, in the absence of mass uprisings, it could also look like a broader and more escalated culture of direct action and attack, anarchist and liberatory ideas spreading more widely, and more autonomous practices being taken up by more people. These are just some examples, and everyone will have their own vision, but the point is that if we wanna become more of a threat, it makes sense to prepare to be treated like one.

We can learn from other countries and contexts, as well as our own, how the state might investigate and respond to something like a prolonged campaign of escalated direct actions and attacks. In those other contexts, when there are no immediate, obvious suspects, the state is forced to investigate in ways that teach us a lot about its resources and how we can mitigate those state responses. Here in Philly, it wasn't so long ago that there was a house raid, which we can assume was attached to a broader

police investigation, that targeted student activists in response to campus solidarity encampments and some light vandalism. So this kind of thing is not hypothetical.

Let's imagine if there were an active investigation going on into an anarchist scene in Philly (or into whatever part of the radical space here feels relevant to you). We'll also imagine that individuals are taking solid precautions around criminalized activities and that there are no obvious suspects for particular incidents. Based on information from elsewhere, this police investigation could look like the following:

1. A first step would be for investigators to geolocate phones to keep track of certain anarchists' locations, who they're meeting up with, etc.
2. Certain people's phones would be wiretapped (not necessarily people who you would expect).
3. A next step would be to plant bugs and/or cameras in anarchist spaces, outside (or inside) anarchists' houses, and/or at known regular meetup spots. GPS trackers are also easy to plant on individuals' cars.
4. A further step would be physical surveillance. This could either be obvious, like occasional police patrols going by your house, and/or the kind that requires some amount of study to reliably detect.[2]

Based on your phone usage, for example, what would the police discover if you were one of the targets of this kind of surveillance? What would they find out about you if one of your friends was targeted? Keep in mind that we can never be completely "secure" and our lack of total security should never allow us to get trapped in inaction. But we should also consider what small

[2]For more information on physical surveillance and how to detect it, see "Measures Against Surveillance",[a] which has examples from Germany.

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

steps we can take now towards better security, for ourselves and our friends' sakes.

Our suggestion is to start by working on your own practices. Try to establish shared practices with your closest people and/or with individuals with whom you already do particular projects. Keep in mind that the level of security you choose for a specific project should depend on the project. For example, organizing a monthly free store in the park will look different from planning a three-person sabotage action. We don't focus on that here because we're trying to keep it short and sweet. But for more information about how to assess the specific security needs of a particular project, see the No Trace Project's "Threat Library".[3]

The following are proposals based on mistakes we ourselves have made or seen elsewhere in anarchist and radical spaces. They're intended to be up for discussion. If you have feedback on these proposals, please email phillysecuritybaseline@riseup.net.

Digital Communication

1) Texting & Calling

A general rule of thumb about this is when texting or talking on the phone (including on Signal), ask yourself, would I want what I'm saying read back to me in a courtroom transcript?

- Do not use Signal to organize anything remotely illegal, including anarchist publication projects or other writing that claims or encourages criminalized activities.
- If you need to, use Signal to schedule in-person meetings or conversations, at which you will then organize what you're trying to organize.

[3] https://notrace.how/threat-library

- Do not hint over Signal about organizing something spicy, that the conversation you're trying to schedule will be spicy, etc. Please just act normal. Leaving out certain details or avoiding certain topics over text can feel uncomfortable at first, but if you keep it up it starts to feel more natural.
- Avoid joining big group chats. If the police arrest someone who is carrying their device, or if they raid a house and seize devices while they're still turned on, they can usually search these devices and this compromises every other individual who is in a group chat with the person whose device was seized. Is it worth it? Consider how you can arrange to get the info on that thread in a different way.

2) Social Media Usage

Social media profiles are either completely public or at the very least extremely easy for law enforcement, fascists, and other adversaries to access. Social media is the first thing cops will go to in order to learn more about local radical or anarchist networks, precisely because it is so easy to access. If you consider that everything you say on social media can be read by law enforcement and is at the very least being passively stored in some data warehouse for later use, it starts to feel very silly to continue handing them info (any kind of info) on a silver platter. Let's make it harder for them! :)

- We recommend not using social media for most projects. For projects with a social orientation, like an anarchist social center or bail fund, sometimes social media can help spread awareness of the project. But social media should not be used to organize, gauge the effectiveness of our organizing, or communicate about radicalism in any other way than posting information about events or projects.
- Consider not having personal social media, since this is such an incredibly easy resource for police investigations.

It hands them a lot of insight into particular individuals' personalities and personal lives, helps them trace social and political networks, charts people's activities, and so on.

Getting rid of social media accounts can feel impossible because it feels like we're sacrificing something that is important for our happiness and well-being, and technically we are—these platforms are designed to get us addicted to the dopamine hits that we get from them. But this isn't just about giving something up, it's also about the possibilities that not using social media offers us. Imagine the worlds we can open up for ourselves once we minimize our use of these alienated digital ways of relating to each other and make more time and space for the happiness and personal well-being that comes from relationships rooted in real connection. Something to think about…

The bottom line: do not talk about other anarchists or anarchist actions on social media. Do not give out any non-public information that would be useful for a police investigation.

Face-To-Face Communication

1) Where We Talk

- Don't discuss illegal actions that have happened, actions that you are planning, or other sensitive information, around phones, or indoors, on your porch, in your backyard, etc.
- Go for a walk, meet in a park, etc.
- When planning more intense actions, try meeting at an agreed-upon spot and then walking somewhere else, ideally to somewhere you haven't been before or don't typically go to.
- Don't make it obvious who you talk about sensitive subjects with (for example, asking someone else to “go for a walk” when you're in the middle of a group of people).

2) What We Talk About

- Don't brag about actions that have happened or imply involvement in actions.
- If you think it makes sense to share sensitive information with someone, try asking them first if they'd like to hear it. It's a disservice to tell someone more than they need to know without their consent. On the off chance that that person is later subpoenaed to a grand jury, or interrogated by law enforcement, it's so much easier for them to say nothing when they genuinely don't know anything.
- Don't discuss involvement in actions after the fact, including with the people you did the action with. Depending on what the action was, a scheduled debrief soon afterwards can be an exception to this. The point is to not casually reminisce, especially months or years later.
- If you're involved in a publication or website that discusses and/or promotes illegal actions, keep your involvement a secret.[4]

Use of Phones/Devices

- Absolutely do not take your phone (or any other networked device, including laptops, networked watches, baby moni-

[4]In the U.S. and elsewhere, there have been cases in which people moderating a website that reposted criminalized actions were charged and served prison time (see for example the SHAC 7 case). There is also now a precedent elsewhere for individuals allegedly involved in anarchist newspaper publications (ones that "reward and justify criminal action") being charged with being in a criminal organization, as well as the publication being used as the jumping off point for an investigation (into widespread attacks) that didn't have any other leads (see writings on the §129 case in Munich such as "Petrol, Printer Ink, and Paranormal Activity"[a]).

[a]https://actforfree.noblogs.org/2025/08/03/about-munich-2019-2025-petrol-printer-ink-and-paranormal-activity

tors, car GPS) to anything at all illegal. Do not bring phones or other networked devices to a conversation in which private or confidential information is shared. Understand that if you do so, you are bringing a potential snitch to the action or conversation. This is very serious.

- Avoid taking your phone to other meet-ups or events at which mapping of social networks (which having your phone there could provide to police) would be helpful to the authorities. For example, radical workshops and presentations, trainings, jail support, etc.
- Consider not bringing your phone when meeting up with friends either, since this obstructs law enforcement's ability to map networks as well and it's always nice to know that none of your opps[5] are listening and learning from you and your friends talking about your private lives, political views, scene drama, etc.
- Many anarchists in Philly have started leaving their phones at home at all times or almost all times, and we encourage this practice to spread further. It is important that there be a broader culture of not taking our phones with us everywhere, so that the few people who already do so don't stand out as much.
- Do not enable biometric authentication (facial recognition, fingerprint) on your devices. The cops can compel you to use this to unlock and gain access to your devices; they can't force you to enter your password.
- Encrypt your phone and laptop, if you have them. Remember that if the device is turned on, encryption will be easy for the cops to bypass. If you're involved in struggles or activities that carry a risk of your house being raided, it should be standard practice to turn off phones and computers before

[5] *No Trace Project note:* Term meaning opponents/enemies.

going to bed. This ensures that they're effectively encrypted and mitigates the seizure of devices during early-morning house raids.

- Do not use unencrypted devices for activities related to anarchy or radical organizing; ideally, don't use unencrypted devices at all.

Reading and Research

- Use Tor Browser to read articles about criminalized activity or articles that are relevant to future actions you might do.
- Consider using a VPN at all times while you're on the internet. We recommend downloading Mullvad VPN; it just runs in the background and you hardly notice it. Using a VPN drastically reduces the ability of adversaries to access your data, even without using Tor Browser.
- Use Tails OS to research illegal actions. Tails leaves no trace of activity on your computer, and forces all internet connections through the Tor network.
- Use Tails OS to moderate sketchy websites.
- If you're interested or already involved in doing more intense actions, and will be using the internet to research these or write/send in communiques about them, you can add additional precautions to using Tails. These are not necessary for everyone, but are a best practice and are especially suitable if you are already known to the police as a radical or anarchist and thus more likely to be under some kind of surveillance at some point.
    - Get a computer in person that you exclusively use for Tails.
    - Make sure you're using a USB stick for Tails that has not been used before or tampered with.

    - Never connect this laptop to your home wifi network —go somewhere else that has internet.[6]

Note that not everyone in an affinity group or constellation has to be doing these tasks, so if your shared resources are limited, just make sure your group has access to at least one of these kinds of computers if you are interested in these kinds of activities.

Writing

- Use Tails for sending communiques.
- Especially for heavier actions, consider not writing a communique if the action seems to speak for itself. Or, write a short communique that is mostly just descriptive and avoids noticeable word choice, slang, writing style, and other potential identifiers. The police use linguistic forensics to plot out who writes what.[7]

Action

- Please do not use a car to travel to an illegal action (unless it was very safely stolen). Use a bike or walk. If it's a less sketchy action, and you're in a city, you can ride transit with

---

[6] According to AnarSec's Tails Best Practices guide,[a] an adversary like the NSA is potentially capable of breaking Tor through a correlation attack. So if you're using wifi at a public space and they do a non-targeted correlation attack, the internet address in that situation won't lead back to you personally. In Jeremy Hammond's case, he was already under surveillance and the state carried out targeted correlation attacks at his home that were then used as corroborating evidence in his case: "Specifically, they correlated Tor network traffic coming from the suspect's house with the times their anonymous alias was online in chatrooms."

[a] https://anarsec.guide/posts/tails-best

[7] See "Who Wrote That?"[a] from Zündlumpen #76.

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

a mask and cash (or try fare evasion!). Sometimes it's useful to carry enough cash on you so you can get a cab if it's an emergency and you need to get outta there.[8]

- There are plenty of resources on how to dress and other precautions to take for going to a rowdy demo or for doing vandalism; for example, see "Baby's First Black Bloc", "A Recipe for Nocturnal Direct Actions",[9] "PRISMA: Primer on Radical Information for Secure Militant Actions",[10] or "A Practical Security Handbook: No Trace Project Edition".[11]
- Read the zine "DNA You Say? Burn Everything to Burn Longer: A Guide to Leaving No Traces"[12] for best practices around not leaving DNA at or near the scene of an action.

Talking to the Cops

- Do not talk to the cops. This one is non-negotiable. This includes being detained during a demo, getting an FBI visit, being interrogated in jail, cops knocking on your door or stopping you in the street asking about something random or unrelated to anarchist activity (in reality it might not be unrelated at all), being approached by the prosecution of a case, being subpoenaed to testify at a grand jury, etc.
- In all cases, tell them you can't talk to them without your lawyer (it's ok if you don't actually have a lawyer). You will probably be required to give your name and birthdate (and

[8]There have been many cases in the U.S. in the past two years alone in which comrades were identified by police as suspects and later convicted in part because they drove a car or motorcycle to the site of the action.

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

[10]https://notrace.how/resources/#prisma

[11]https://notrace.how/resources/#security-handbook-2

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

possibly your address) when arrested and that's fine. If it's an FBI visit, ask for their card.

- Afterwards, contact Up Against the Law or another local anti-repression group and then discuss with your comrades if it makes sense to put out information about the incident to others in your networks. Not every interaction with the police needs to lead to a public statement (for example, traffic stops, apolitical arrests, mass demo arrests, and so on), but in the case of an FBI visit, grand jury subpoena, or any other attempted interrogation by law enforcement, it's usually good to spread this information far and wide as it is likely linked to a broader investigation into your networks. Discuss what the police asked and how they asked it; what, if anything, would be interesting for others in struggles to know about; and, if so, how this info can be circulated to other comrades. This also reduces the isolation of being singled out by the law, which can feel much worse if you feel alone in it. This brings us into our next and final topic…

Discussing Repression

- The state knows who got arrested and what the charges are; it knows that the FBI visited your home, that someone got a subpoena for a grand jury, and so on. Basic information about repression and police investigations should be shared widely so other people are aware of what level of attention anarchists are attracting from law enforcement and can move accordingly.
- Pretty much all information that is in the cops' and prosecution's hands (for example, what is written in the affidavit of probable cause for an arrest) is ok to be shared with others. When you describe why someone got arrested, make sure you are referring to the state's information about

it, or to something you read in the news ("The cops are saying that…", "The defendant allegedly did…", "I read that…", etc.) Don't speak from your personal experience and don't say that the accused person did something illegal, just that they are accused of doing it.

- Do not speculate about why someone might have gotten a particular charge, etc. Be content that you don't know anything and could honestly say to the cops that you can't tell them anything if for some reason you were questioned about the situation.
- If for some reason law enforcement interrogated you or asked you questions about an anarchist scene in Philadelphia, specific individuals, etc, it is your responsibility to inform other anarchists about the interrogation. There is no reason not to do this unless you gave them information in the course of that conversation and are trying to cover that up. If you didn't answer their questions, there's no reason not to let other people know about the conversation.

Case Studies for Further Reading

- "No Bars: Bringing Down the Techno-Prison"[13]
- "Cops and Robbers? A History of Investigative Techniques"[14]
- "Green Scared?"[15] by Rolling Thunder

[13]https://rupture.noblogs.org/post/2002/10/04/no-bars
[14]https://notrace.how/resources/#cops-and-robbers
[15]https://notrace.how/resources/#green-scared

In this text, we try to identify specific needs, for example for various kinds of communication with each another, and establish some baseline practices around meeting those needs that we can all share to make ourselves harder targets for state repression. […] We can empower ourselves to keep fighting for anarchy and liberation by establishing some shared practices in the Philadelphia anarchist/radical space that make us all safer.

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.