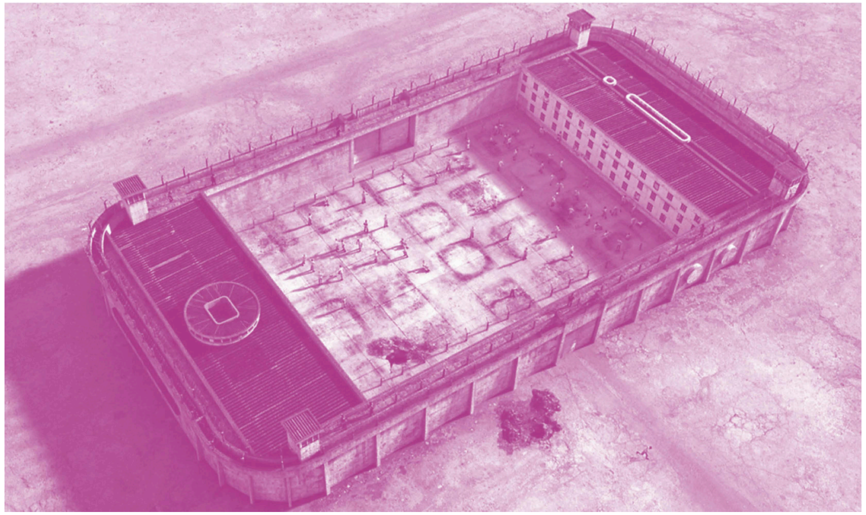
Effective security culture and operational security prevents the forces of repression from knowing about our specific criminal activities, but also about our lives, relationships, movement patterns, and so on. This knowledge is a huge advantage in narrowing down suspects and conducting targeted surveillance. This article will outline some strategies for killing the cop in your pocket.

```
 ,-\__
 |f-"Y\  -------------------
 \()7L/ < Be gay, do crime! >
  cgD    -------------------    __ _
  |\(                \         .'  Y '>,
   \ \                \       / _   _   \
    \\\                \      )(_) (_)(|}
     \\\                      {  4A   } /
      \\\                      \uLuJJ/\l
       \\\                     |3    p)/
        \\\___ __________      /nnm_n//
        c7___-__,__-)\,__)(".  \_>-<_/D
                   //V     \_"-._.__G G_c__.-__<"/ ( \
                          <"-._>__-,G_.___)\   \7\
                         ("-.__.| \"<.__.-" )   \ \
                         |"-.__"\  |"-.__.-".\   \ \
                         ("-.__"". \"-.__.-".|    \_\
                         \"-.__""|!|"-.__.-".)     \ \
                          "-.__""\_|"-.__.-"./      \ l
                           ".__""">G>-.__.-">       .--,_
                               ""  G
   _  _
__| || |__ _____    ____  _____    ___________ ____  ____  #tech
\   __   / \__   \  /    \ \__   \  /  __/  ___// __ \/ ___\ #guides
 |  ||  |   / __ \|   |  \ / __ \|   | \___ \\  ___/  \__  #for
/_  ~~  _\ (____  /___|  /(____  /___| /____/ \___\ \____\ #anarchists
  |_||_|        \/     \/      \/
```

Kill the Cop in Your Pocket



Series: Defensive

This version of the zine was last edited on 2024-04-23. Visit anarsec.guide to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for it. Ai ferri corti.

AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

Defensive

Tails

- Tails for Anarchists
- Tails Best Practices

Qubes OS

- Qubes OS for Anarchists

Phones

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

General

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Offensive

Coming soon

Contents

Effective security culture and operational security[1] prevents the forces of repression from knowing about our specific criminal activities, but also about our lives, relationships[2], movement patterns, and so on. This knowledge is a huge advantage in narrowing down suspects and conducting targeted surveillance. This article will outline some strategies for killing the cop in your pocket.

Your phone's location is tracked at all times[3], and this data is harvested by private companies, allowing police to bypass needing to obtain a warrant. The phone's hardware identifiers and subscription information[4] are logged by each and every cell tower your phone connects to. Hacking services like Pegasus[5] put total phone compromise within reach of even local law enforcement and are "zero-click," meaning they don't depend on you clicking a link or opening a file to hack your phone. On the flip side, after more than 30 arsons in a small town in France went unsolved, investigators complained[6] that "it is impossible to make use of phone or vehicle registration data because they operate without phones or cars!"

Encryption and Geolocation

In a recent repressive operation[7] against an anarchist, the police tracked the geolocation of the suspect's flip phone in real time and made a list of everyone the suspect had called. It is well known that surveillance like this is not uncommon, and yet many comrades carry

[1] notrace.how/resources/read/csrc-bulletin-1-en.html#header-a-base-to-stand-on-distinguishing-opsec-and-security-culture

[2] notrace.how/threat-library/techniques/network-mapping.html

[3] vice.com/en/article/m7vqkv/how-fbi-gets-phone-data-att-tmobile-verizon

[4] anonymousplanet.org/guide.html#your-imei-and-imsi-and-by-extension-your-phone-number

[5] amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[6] actforfree.noblogs.org/post/2022/04/17/grenoblefrance-these-saboteurs-of-the-ultra-left-have-been-elusive-for-five-years/

[7] notrace.how/resources/#ivan

a cell phone with them wherever they go, or make unencrypted calls to other anarchists. We believe that both of these practices should be avoided. Let's not make the job of the police and intelligence agencies so easy by handing them our social networks and geolocation history on a silver platter.

If you don't leave the house with a phone, the police will have to resort to physical surveillance to determine your whereabouts, which is resource-intensive and detectable. If you are ever placed under physical surveillance, the investigator's first step is to understand your "movement profile," and your phone's geolocation history provides a detailed picture of your daily patterns.

Some anarchists respond to the problems with smartphones by using flip phones or landlines to communicate with each other, but these devices do not support encrypted communication†, so the State learns who is talking to whom and what they are talking about. A primary goal of targeted surveillance is to map the target's social network in order to identify other targets. The only way to avoid giving this information to our enemies is to use only encrypted mediums[8] to communicate with other anarchists through technology.

Metadata Patterns

The normalization of constant connectivity within dominant society has led some anarchists to correctly note that phone metadata† is useful to investigators. However, the conclusion that some draw from this insight, that we should "never turn off the phone,"[9] takes us in the wrong direction. Their logic is that your interactions with technology form a baseline metadata pattern, and moments that deviate from this baseline become suspicious if they coincide with when an action occurs, which can be used by investigators to narrow down suspects.

[8] anarsec.guide/posts/e2ee/

[9] web.archive.org/web/20210126183740/https://325.nostate.net/2018/11/09/never-turn-off-the-phone-a-new-approach-to-security-culture

While this is true, the opposite conclusion makes far more sense: anarchists should minimize the creation of metadata patterns that investigators would have access to.

Our connections to the infrastructures of domination must remain opaque and unpredictable if we are to retain our ability to strike the enemy. What if the reconnaissance required for an action involves an entire weekend away from electronic devices? Or let's start with the simple fact that phones must be left at home during an action — this only becomes the outlier to a pattern if phones otherwise accompany us wherever we go. In a normatively "always connected" life, either of these metadata changes would stick out like a sore thumb, but this is not the case if you refuse to be constantly plugged in. **To minimize your metadata footprint, you must leave your phone at home by default**.

Do You Really Need a Phone?

Phones have colonized everyday life because people have been instilled with the belief that they need *synchronous* communication in every moment. *Synchronous*† means that two or more parties communicate in real time, as opposed to something *asynchronous*† like email, where messages are sent at different times. This "need" has become normalized, but it is worth resisting within the anarchist space. Anarchy can only be anti-industrial[10]. We must learn to live without the conveniences sold to us by the telecom companies, we must defend (or rekindle) our ability to live without being connected to the Internet at all times, without algorithmic real-time directions, and without the infinite flexibility to change plans at the last minute.

If you decide to use a phone, in order to make it as difficult as possible for an adversary to geotrack it, intercept its messages, or hack it, use GrapheneOS[11]. If we can agree to **only use encrypted**

[10] theanarchistlibrary.org/library/bismuto-beyond-the-moment#toc1

[11] anarsec.guide/posts/grapheneos/

possible for your service provider and possibly other parties to know where your device is at any given time).

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting". The Tor network can be accessed through the Tor Browser on any operating system. The Tails[†] operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[44] and Privacy Guides[45]. To understand the limitations of Tor, see the Whonix documentation[46].

Two-Factor Authentication (2FA)

Two-factor authentication (or "2FA") is a way for a user to identify themselves to a service provider by requiring a combination of two different authentication methods. These can be something the user knows (such as a password or PIN) or something the user has (such as a hardware token or mobile phone).

VoIP (Voice over Internet Protocol)

Google Voice is a well-known and insecure VoIP service; this technology routes your calls over the Internet (as Signal does) instead of using standard cell tower transmission. Unlike Signal, VoIP allows you to receive calls from anyone, not just other Signal users. The advantage of using VoIP for calls over a data plan is that you can create different numbers for different activities (one for bills, one for signing up for a Signal account, etc.), and you never need to turn off Airplane mode. The advantage of using a data plan instead is that you can use it away from Wi-Fi, at the cost of geolocation (i.e. it will be

[44] anarsec.guide/posts/tails/#tor

[45] privacyguides.org/en/advanced/tor-overview/

[46] whonix.org/wiki/Warning

communications[12] to communicate with other anarchists, this rules out flip phones and landlines. GrapheneOS is the only smartphone operating system that provides reasonable privacy and security.

To prevent your movements from being tracked, treat the smartphone like a landline and leave it at home when you are out of the house. Even if you use an anonymously purchased SIM card, if it is linked to your identity in the future, the service provider can be retroactively queried for geolocation data. If you use the phone as we recommend (as a Wi-Fi only device[13] that is kept in airplane mode at all times), cell towers won't be able to connect to it. It's not sufficient to only leave the phone at home when you're going to a meeting, demo or action because that will be an outlier from your normal pattern of behaviour and serve as an indication that criminal activity is taking place in that time window.

You may choose to live without phones entirely, if you don't feel that you need an "encrypted landline". The strategies for minimizing the need for phones that follow rely on computers, where synchronous communication is also possible but more limited.

Bureaucracy

Many bureaucratic institutions that we are forced to deal with make it difficult to live without a phone: health care, banking, etc. Communicating with bureaucracies doesn't need to be encrypted, so you can use a Voice over Internet Protocol (VoIP)[†] application. This allows you to make phone calls over the Internet rather than through cell towers.

Any VoIP application that is available on a computer is asynchronous because it doesn't ring when the computer is off — you rely on the voicemail feature to return missed calls. For example, a service like

[12] anarsec.guide/posts/e2ee/

[13] anarsec.guide/posts/grapheneos/#what-is-grapheneos

jmp.chat[14] gives you a VoIP number, which you can pay for in Bitcoin, and you make calls using an XMPP application — Cheogram[15] works well.

Though usually more expensive than VoIP, a flip phone or landline also works well for making and receiving ‘bureaucratic’ calls from home, like those mentioned above.

VoIP usually works for any two-factor authentication[†] (2FA) you need (when a service requires you to receive a random number to log in). Online phone numbers[16] are another option.

Communication

Not carrying a phone everywhere requires a change in the way you socialize if you are already caught in the net[17]. Being intentional about minimizing the mediation of screens in our relationships is a valuable goal in and of itself.

Using an “encrypted landline” to make phone calls and a computer for encrypted messaging allows us to avoid the unending stream of notifications on a device that is always within reach.

It would do us all good to take a hard look at the monoculture of Signal group chats that have replaced face-to-face encounters in some parts of the anarchist space. This capture of organizing relationships by smartphone culture forces us into a never-ending meeting that is relatively easy to surveil.

That said, encrypted communication can be useful to set a date and time to meet, or for projects shared across distances. See Encrypted

[14] kicksecure.com/wiki/Mobile_Phone_Security#Phone_Number_Registration_Unlinked_to_SIM_Card

[15] cheogram.com/

[16] anonymousplanet.org/guide.html#online-phone-number

[17] theanarchistlibrary.org/library/return-fire-vol-4-supplement-caught-in-the-net

and iOS. Linux and some versions of Android are the only open-source options on this list.

Synchronous communication

Unlike asynchronous communication[†], both parties must be online at the same time. This does not require servers for the communication and is often referred to as “peer to peer”.

Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals[35], and vulnerabilities[35], and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable event that can be malicious (such as a DDoS attack[35]) or accidental (such as a hard drive failure). Threat modeling is the deliberate activity of identifying and assessing threats and vulnerabilities.

For more information, see the No Trace Project Threat Library[40], Defend Dissent: Digital Threats to Social Movements[41] and Defending against Surveillance and Suppression[42].

Tor network

Tor[43] (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

[40] notrace.how/threat-library/

[41] open.oregonstate.education/defenddissent/chapter/digital-threats/

[42] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/

[43] torproject.org/

End-to-end encryption (e2ee)

Data is encrypted[35] as it travels from one device to another — endpoint to endpoint — and cannot be decrypted by any intermediary. It can only be decrypted by the endpoints. This is different from "encryption at rest", such as Full Disk Encryption[35], where the data stored on your device is encrypted when the device is turned off. Both are important!

For more information, check out Encrypted Messaging for Anarchists[36], and Defend Dissent: Protecting Your Communications[37].

Metadata

Metadata is data that provides information about other data. For example, a JPG file contains the actual image (data) but it may also contain metadata such as the date the file was created, the type of camera, GPS coordinates, and so on. Metadata can be valuable to attackers (to find appropriate exploits for outdated software the target is using), government agencies (to collect information about people to create social graphs), and other parties (to target location-based advertising). Whenever you use a computer, you are likely leaving metadata behind.

For more information, see Remove Identifying Metadata From Files[38] and Defend Dissent: Metadata[39].

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android,

[35] anarsec.guide/glossary

[36] anarsec.guide/posts/e2ee

[37] open.oregonstate.education/defenddissent/chapter/protecting-your-communications/

[38] anarsec.guide/posts/metadata

[39] open.oregonstate.education/defenddissent/chapter/metadata/

Messaging for Anarchists[18] for various options appropriate to an anarchist threat model[†].

Emergency Calls

A passerby on the street will often lend you their phone to make an urgent call if you tell them that yours is out of battery. To receive emergency calls, if you cannot be reached as described above, we can stop by each other's houses or arrange encrypted messaging check-ins in advance. What scenarios actually require you to be available to receive a call at any moment? If these actually exist in your life, you can organize around them without projecting that urgency into all other areas and moments.

Directions

Buy a paper map of your area and bring it with you. For longer trips or trips where you need directions, use OpenStreetMap[19] to note them ahead of time.

Music and Podcasts

They still make MP3 players! For a much lower price, you can play music and podcasts, but the device has no GPS or radio hardware. However, that doesn't mean you can't be geolocated by an MP3 player. If it connects to Wi-Fi, your MP3 player's approximate location can be determined from its IP address.

Appendix: Against the Smartphone

[18] anarsec.guide/posts/e2ee/

[19] openstreetmap.org/

From Fernweh (#24)[20]

It's always with us, always on, no matter where we are or what we're doing. It keeps us informed about everything and everyone: what our friends are doing, when the next subway leaves, and what the weather will be like tomorrow. It takes care of us, wakes us up in the morning, reminds us of important appointments, and always listens to us. It knows everything about us, when we go to bed, where we are and when, who we communicate with, who our best friends are, what music we listen to, and what our hobbies are. And all it asks for is a little electricity now and then?

When I stroll through an area or take the subway, I see it with almost everyone, and no one can last more than a few seconds without frantically reaching for their pocket: the cell phone is whipped out, a message is sent, an email is checked, a photo is liked. It is put away again, a short break, and here we go again, skimming through today's news and checking out what all the friends are up to…

It's our companion when we're on the toilet, at work or at school, and it apparently helps to fight boredom while we're waiting or working, etc. Is this perhaps one of the reasons for the success of all these technological devices, that real life is so damn boring and monotonous that a few square centimeters of screen is almost always more exciting than the world and the people around us? Is it like an addiction (people definitely have withdrawal symptoms…) or has it even become part of our body? Without it, we no longer know how to orient ourselves and feel that something is missing? So it is no longer just a tool or a toy, but a part of us that also exerts a certain control over us, to which we adapt, for example, by not leaving the house until the battery is fully charged? Is the smartphone the first step in blurring the line between human and robot?

When we see what technocrats of all kinds are prophesying (Google Glasses, implanted chips, etc.), it almost seems as if we are heading

[20] fernweh.noblogs.org/texte/24-ausgabe/gegen-das-smartphone/

> **Operating system†**: **Qubes OS** has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials[30]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[31].

See When to Use Tails vs. Qubes OS[32]. We do not offer "harm reduction" advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists[33]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[34].

Appendix: Glossary

Asynchronous Communication

Unlike synchronous communication†, both parties do not need to be online at the same time. This relies on some sort of server to store messages until the message recipients come online. This is the type of messaging that most people are familiar with (email, Signal, etc.).

[30] anarsec.guide/posts/linux

[31] anarsec.guide/posts/qubes/

[32] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

[33] anarsec.guide/posts/e2ee/

[34] anarsec.guide/posts/tamper/

and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which “private or confidential words are spoken” and must remain so, even if it’s switched off, we become a potential state informer…”

You may also be interested in the Threat Library’s “Digital Best Practices”[25].

Your Phone

Operating system†: GrapheneOS is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[26]. If you decide to have a phone, treat it like an “encrypted landline” and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[27].

Your Computer

Operating system†: Tails is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network†. See Tails for Anarchists[28] and Tails Best Practices[29].

[25] notrace.how/threat-library/mitigations/digital-best-practices.html

[26] anarsec.guide/posts/grapheneos/

[27] anarsec.guide/posts/nophones/

[28] anarsec.guide/posts/tails/

[29] anarsec.guide/posts/tails-best/

towards becoming cyborgs, people with implanted smartphones that we control through our thoughts (until our thoughts themselves are finally controlled). It is not surprising that the media, the spokesmen of domination, show us only the positive aspects of this development, but it is shocking that almost no one questions this view. It’s probably every ruler’s wildest dream: to be able to monitor everyone’s thoughts and actions at all times and to intervene immediately in case of any disturbance. Totally controlled and monitored worker bees who are allowed to have some (virtual) fun as a reward while a few profit.

With the vast amounts of data now so readily available from anyone and everyone at any time of day, social control and surveillance has also reached a whole new level. This now goes far beyond tapping cell phones or sifting through messages (as during the 2011 UK riots). With access to an incredible amount of information, intelligence agencies are able to define what is “normal.” They can determine which locations are “normal” for us, which contacts are “normal,” etc. In short, they can quickly establish and almost in real time if people are deviating from their “normal” behavior. This gives some people enormous power, which is used whenever there is an opportunity to take advantage of that power (i.e. to surveil people). Technology is part of power, it comes from power and needs power. It takes a world in which people have extreme power to enable the production of something like the smartphone. All technology is a product of the current oppressive world, is part of it, and will reinforce it.

In today’s world, nothing is neutral. To date, everything that has been or is being developed is designed to extend control and to make money. Many of the innovations of recent decades (such as GPS, nuclear power, or the internet) even come directly from the military. Most of the time these two aspects go hand in hand, but the “welfare of mankind” is certainly not a motivation, especially when it is developed by the military.

Perhaps taking the example of architecture can better illustrate something as complex as technology: let’s take an empty and disused prison, what should be done with this structure except to tear it down? Its very architecture, its walls, its watchtowers, its cells, already contain the purpose of this building: to imprison people and destroy them psychologically. It would be impossible for me to live there, simply because the building is oppressive.

It is the same with all the technologies of today that are presented to us as progress and as something that makes life easier. They were designed with the intention of making money and controlling us, and will always carry that. No matter how many supposed benefits your smartphone brings you, those who get rich by collecting your data and monitoring you will always benefit more than you.

If in the past it was said that "knowledge is power", today it should be said that "information is power". The more rulers know about their flocks, the better they can dominate them — in this sense, technology as a whole is a powerful tool of control to predict and thus prevent people from coming together to attack what oppresses them.

These smartphones seem to need a little more than just a little electricity… In our generation, which at least knew a world without smartphones, there might still be some people who understand what I'm talking about, who still know what it's like to have a discussion without looking at their phone every thirty seconds, to get lost and discover new places by doing so, or to debate something without immediately asking Google for the answer. But I don't want to go back to the past, even though it wouldn't be possible anyway, but the more technology penetrates our lives, the harder it becomes to destroy it. What if we are one of the last generations able to stop this evolution of human beings into completely controlled robots?

And what if at some point we will be unable to reverse this development? Humanity has reached a historically new stage with technology. A stage where it is able to annihilate all human life (nuclear energy) or to modify it (genetic manipulation). This fact underlines once again the need to act today to destroy this society. To

do this, we need to encounter other people and communicate our ideas.

Isn't it obvious that if instead of talking to each other, we only communicate in messages of five sentences or less, there will be long-term effects? Apparently not. First of all, the way we think influences the way we speak, and vice versa — the way we speak and communicate influences the way we think. If we are only able to exchange the shortest and most concise messages, how can we talk about a completely different world? And if we can't even talk about another world, how can we reach for it?

Direct communication between autonomous individuals is the basis of any shared rebellion, it is the starting point of shared dreams and common struggles. Without unmediated communication, a struggle against this world and for freedom is impossible.

So let's get rid of the smartphones and meet face to face in an insurgency against this world! Let's become uncontrollable!

Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[21] for the purposes of incrimination[22] and network mapping[23]. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France[24]: "So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone

[21] notrace.how/threat-library/techniques/targeted-digital-surveillance.html

[22] notrace.how/threat-library/tactics/incrimination.html

[23] notrace.how/threat-library/techniques/network-mapping.html

[24] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/