

MOBILE PHONE SECURITY FOR ACTIVISTS AND AGITATORS



HÅKAN GEIJER

2026 EDITION

Some of the most powerful tools at our disposal are our internet connected smart phones. Instant communication and the sum of all human knowledge at our fingertips massively increases our ability to affect the world around us. But this connectivity comes at the cost of increased surveillance by corporations, State security apparatuses, and private individuals. Those who are active in liberatory movements are generally aware of this surveillance, and collectively we have developed privacy practices and an internal security culture to counter disruptions to our efforts to organize for a more egalitarian and autonomous future.

There are many urban legends around phone use that stem from inaccurate understandings of the technologies that comprise and are used by phones as well as what capabilities the State and private actors have at their disposal to surveil individuals via their phones. Threat modeling is the process of identifying threats and building specific and pragmatic countermeasures against them, but without accurate models of one's adversaries, such models lead to ineffective and insufficient countermeasures.¹ Action taken based off misinformation can more easily lead to arrest or create the impression of an all-seeing adversary thus stifling action. This zine covers the basic technologies of phones and addresses common urban legends so that you and your comrades can resist disruption and organize effectively.

There is no such thing as perfect security, and security is subjective. It is not a binary that is either "on" or "off," nor is it even a universal spectrum between "better security" and "worse security." Security is best discussed as "more secure under these conditions against those threats." What might be effective for keeping the State from tracking your location via your phone might be useless for keeping an abusive partner from reading your messages. This guide will help you understand the risks you face so you can make informed decisions. Security culture is not a guarantee of safety, but its necessary norms and habits reduce the harms we face. It may prevent your imprisonment or save your life, or do so for those around you.

This zine was written in mid 2026 by anarchists in Europe and North America,² and as such this knowledge will be most relevant to those close to us in both space and time. We intentionally omit (most) legal considerations; just because your adversary isn't allowed to do something doesn't mean they won't do it anyway. We instead focus on what is technically possible. We also acknowledge the biases we can't see past (they can still be found in this zine), and we are not able to predict the future. You will have to use the knowledge of your personal and local contexts to adapt what is written here to the specific threats you face.

¹What threat modeling is and how to do it well can be a complex subject, but a bit of basic observation, research, and critical thinking will get you most of the way there. If you want to read in depth about the topic as it applies to radicals and activists, see the zine *Threat Modeling Fundamentals* available at opsec.riotmedicine.net.

²The original was written in early 2022. This is an update.

YOUR PHONE AND YOU

Your phone³ is not merely a valuable personal possession. It is an extension of yourself. It contains your memories, your knowledge, your private and semi-private thoughts, as well as those of the people you communicate with. It enables you to rapidly look up information and share it with others. This connectivity and access to knowledge makes us more effective as we pursue our goals. Phones have in some ways become requirements to function in modern society. Because of this, individuals are rarely without them. When its battery dies or we leave home without it we can feel naked, incapacitated, or like some part of us is missing.

An adversary seizing a phone or infecting it with malware can be disastrous. They could have access to all the currently logged-in accounts on your phone as well as photos, messages, e-mails, and notes. Installed malware or stalking apps could enable your phone's microphone or real-time location tracking after it's returned to you. Aside from these types of active surveillance, your phone provides passive surveillance to third parties such as police, corporations, and even private individuals who can request or buy real-time access to metadata in bulk that is available through your carrier, ISP,⁴ or advertising brokers.

Because of these possibilities of surveillance, activists rightly say "Your phone is a cop" and "Your phone is a snitch." So then, should we keep using our phones of the many benefits they provide, or should we discard them because of the dangers they pose? Or, perhaps there's some nuance in when and how we can use phones that allows us to retain much of their benefit while evading much of their detriments. This is best seen when looking at trade-offs. We could ditch our phones and lose a means of surveillance, but we'd also lose a means of instant communication. What does a neighborhood antifascist watch gain by using encrypted phones versus nothing? Could you mobilize rapid response to police raids without mobile phones given that your comrades are often busy with multiple jobs or not at places with a known landline number? Is it even possible to warn someone that cops might be coming for them if you'd have to ride your bike to their house and knock on their door? Many advocates of



We are all already Donna Haraway's cyborgs, unfortunately including all the dystopian cyberpunk features of fusing ourselves to corpo controlled machines while existing under capitalism.

³To save space, we are using "phone" to mean "mobile phone" or "cell phone."

⁴Internet service provider.

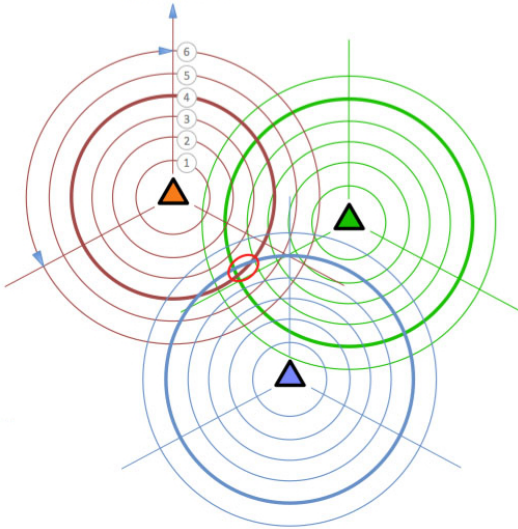
a phoneless existence point to excess social media use facilitated by these phones or a theoretical mass malware infection of every activist where every single phone is a hot mic, but these claims do not reflect our reality.

Phones offer us many advantages as activists, and carrying out common activities in our everyday life would become incredibly burdensome without them, sapping time and energy we might otherwise put toward our broader goals. Let's then carefully look carefully at how we can use phones with increased safety.

PHONE TECH

In order to understand how phones can be compromised and used to spy on and surveil you, we need to have an accurate understanding of how different technologies work, such as a phone's hardware, its firmware, and its operating system as well as mobile networks and to some extent the internet at large. This will help you build a threat model so you can make informed decisions, which is preferable to memorizing seemingly arbitrary steps.

CELLULAR NETWORKS



Cellular networks take their name from the many overlapping cells of coverage provided by transceiver⁵ towers or antennas.⁶ In urban areas, there is more dense coverage, so a single phone is in contact with more towers. In suburban and rural areas, there is less overlap, and consequently a phone is in contact with fewer towers.

Network operators can use information about the signal itself to estimate phone locations. Coarse location can be determined by the angle-of-arrival at the tower or by knowing from which sector⁷ the signal arrived. When a phone's distance from multiple towers is simultaneously measured, the network

⁵Transmitter/receiver.

⁶Not all cellular sites are towers, but this text will use the layperson term for brevity. The term base station is also frequently used.

⁷The cone-shaped area covered by a single antenna.

provider can triangulate the phone's location very accurately.⁸ Older LTE networks can position a phone's position to within a few dozens meters, and modern 5G networks are able to do this to within 5 meters. The more towers there are, the more reliably a phone's location can be determined, thus rural triangulation is generally less accurate than urban triangulation.

When phones connect to a cellular network, they send a unique device ID (IMEI⁹) along with their subscriber's ID (IMSI¹⁰). An IMSI is typically stored either on a physical SIM¹¹ card or eSIM.¹² This means that swapping multiple SIM cards between a device or one SIM card between multiple devices can create a hard link between these identities. A valid SIM or IMSI is not required to make a phone call; these only authenticate the device to the carrier and determine if the device is permitted to make calls or use mobile data. For example, in most (if not all) regions, emergency services can be called without a SIM. Thus, removing a SIM card from your phone **does not** prevent tracking.

TYPES OF PHONES

Most people who say “phone” mean “smart phone,” namely one with an operating system and apps that can be installed by users. Besides smart phones there are devices like the early “bricks” and flip phones that can only send and receive calls and SMS messages up to feature phones that have very rudimentary e-mail clients and web browsers. We'll refer to these other non-smart phones as “simple phones.”¹³

SMART PHONES

Smart phones generally have a location service feature that allows the phone to provide high-accuracy, real-time location data to applications, most notably maps. The location service primarily uses signals received from GPS,¹⁴ GLONASS,¹⁵ or similar satellites to triangulate the phone's position, but they also use A-GPS¹⁶ which combines received cell tower signals, WiFi signals, and even data exchanged over the internet to quickly and more accurately calculate a phone's position.

Smart phones often also contain a compass, accelerometer, gyroscope, and barometer. Even without GPS, A-GPS, or signal from cell towers, measurements from these sensors can be combined to derive a current location from a known previous location.

⁸This is called “uplink multilateration.” And as a note, we're using the common term “triangulation” to mean “multilateration” because in this case it's worth trading technical accuracy for understandability.

⁹International Mobile Equipment Identity.

¹⁰International Mobile Subscriber Identity.

¹¹Subscriber Identity Module.

¹²Embedded-SIM. A chip integrated directly into the device or a virtual SIM within an app.

¹³Some people use the phrase “dumb phone” to mean either all simple phones or just bricks and flip phones, so we are intentionally avoiding this phrase for clarity.

¹⁴Global Positioning System, run by the US Department of Defense.

¹⁵Global Navigation Satellite System, a GPS alternative run by the Russian Roscosmos.

¹⁶Assisted GPS.

What this means is that if your phone is on airplane mode and not sending signal, apps or malware might still be tracking your location and could send it when signal is restored. Likewise, disabling location services or even putting your phone in Faraday bag that blocks all signal and then carrying it with you might still allow your location to be coarsely determined. That said, utilizing airplane mode with WiFi and Bluetooth disabled is better than not, as is using a Faraday bag rather than not (these are discussed later).

SIMPLE PHONES



#nostalgia

Some activists believe that using simple phones rather than smart phones is “more secure.” Because a phone without GPS or location services can still be geolocated, simple phones do not offer significant protection from location tracking. Even these simple phones typically lack widely available text or voice chat apps, which means that only unencrypted SMS and telephone calls are available, and these are susceptible to interception in more ways than if they had even the most basic encryption. Some simple phones may only have 2G capabilities which means that calls and SMS are trivially interceptable with only about €25 worth of consumer-grade equipment. Many of these devices may have hidden internet capabilities that send telemetry data back to manufacturers without users being aware.

Simple phones may have less features which leads some to believe there are fewer ways to hack them. Simple phones have been hacked for decades and they continue to be hacked. This is in part because there is little economic incentive for independent researchers to find vulnerabilities nor for the companies to expend resources on keeping low-margin devices updated.

Similarly, don’t forget that in 2024, Mossad operatives targeted Hamas and detonated explosives in walkie-talkies and pagers killing 42 and injuring upwards of 4,000, many of which were civilians and noncombatants.¹⁷ This was possible because they’d inserted themselves into the supply chain.

Simply put, **simple phones are not more secure than smart phones** against the majority of threats that most activists face.

MALWARE

Malware is short for “malicious software.” It is a program that does something you don’t want and tries to hide its activities. Malware created by the State can have various goals and targets, but usually it is installed directly or remotely onto phones, laptops, and even other electronics like WiFi routers in order to monitor everything that connects to them and what traffic moves through them.

¹⁷Why yes, this is a fucked up war crime.

Outdated internet security training says that malware is installed by visiting dodgy websites or opening attachments on e-mails from unknown recipients, and while this can still be true, the ways and opportunities to infect a phone have grown with the ubiquity and complexity of the technologies around us. Most, if not all, of your apps poll for notifications or wait for notifications to arrive from Google or Apple notification services and then make requests to the app's servers. Some malware is zero-click meaning that it requires no user interaction in order to infect a device. As an example, the Pegasus spyware suite from the NSO Group uses zero-click exploits and has targeted activists, journalists, and politicians. Malware can be installed on your phone even if you only use trusted apps and only (knowingly) accept messages from trusted contacts.

Some malware only stays in your phone's memory while your phone is on and is unable to persist across reboots. Because of this, some malware will hijack the phone's shutdown routine and do a false shutdown. Still, periodically rebooting your phone has the potential to clear malware.

If you have credible evidence that suggests your phone has been compromised, you will need to find a malware specialist who can help you investigate this. Your slightly techy friend is probably not expert enough to meaningfully examine your phone. You will most likely find help from activist NGOs such as Access Now, Amnesty International, the EFF, or similar.

You may need to get a new device, or at the very least perform a factory reset as this will clear most malware from the device. Malware is less common than you think, but don't let its uncommon nature cause you to ignore legitimate warning signs. State-sponsored malware will not be as readily detectable as low-effort malware, so the common methods may not apply. Detection is unfortunately not something you can do yourself.

OPERATING SYSTEMS

One of the most common questions activists ask about smart phones is "Which is more secure, iOS or Android?" As with all security questions, the answer is "it depends."

Smart phone operating systems (OSes) come in two main flavors: iOS for Apple devices and Android for everything else. iOS is proprietary which means its source code is a trade secret. Android is an OS based on Linux with public source code that manufacturers adapt to their devices. Unfortunately, they usually add proprietary components with private source code. In addition, there are several versions of Android maintained by the open source community,¹⁸ most notably LineageOS and GrapheneOS. The latter is very security and privacy focused but is notorious for being only available on Google Pixels, though in a press release from earlier this year,

¹⁸It should be nevertheless noted that when using a community maintained version of Android, the phone may still send telemetry data or be exposed to tracking by Google or other companies because of features in the OS like the Google Play Store or weather services or apps like GMail or Instagram.

upcoming support for Motorola devices was announced.

When a phone is powered on, the hardware starts a bootloader using a process where each step verifies the integrity of the software needed for the next step up to the point where the operating system starts and opens a login screen. This goes by various names such as secure boot or verified boot. In order to install a custom OS, this verified boot process must be temporarily disabled, otherwise the hardware would refuse to load the new OS because it is not cryptographically signed by the trusted key that was included by the original equipment manufacturer. This allows for the possibility of a malicious OS that could read your data being installed instead of the genuine OS, either by physical access or by malware. This does not, however, mean that stock OSes are more or less secure than custom OSes. It means that there is a different risk profile when disabling verified boot and using a custom OS.

When malware is developed, it must target a single application or OS. Developing malware is expensive and time-consuming, moreso to make a suite that can target many applications or OSes. Once malware is deployed, it can be detected and rendered unable to infect new devices by updates to the targeted app or OS.¹⁹ Because of this, it is more economical to write malware that can target many users. While this makes iOS a lucrative target for malware developers relative to the diversity of the Android ecosystem, the diversity of Android comes with a lack of quality controls and the increase potential for (accidental) obsolescence that can lead to devices being very easy to exploit. This can mean smaller phone manufacturers doing shoddy development or stopping updates for a certain phone model to “encourage” users to buy a newer one. Or, it can mean open source projects being abandoned due to lack of contributors.

Our recommendations are as follows:

- For most individuals who are trying to avoid mass surveillance and low-effort hackers, up-to-date iOS or stock Android from major phone manufactures are sufficient as they are easiest to use and reasonably secure.
- For individuals who are significantly involved in social movements or expect to be individually targeted, at this time we recommend for their organizing and political work that they use GrapheneOS without Google Play Services, use F-Droid as the sole app repository, and install only the minimum number of apps required for communication.
- For individuals who have attracted or expect to attract the attention of intelligence agencies, phones should be avoided for anything related to activism.²⁰

¹⁹Additionally, malware has the interesting property that when used it can be captured and cloned so that others can reuse it. This would be like if every time a missile landed on enemy territory, there would be a chance it could be instantly copied and infinitely reproduced. It would also mean that particular type of missile would be much easier to intercept in the future. Militaries would be hesitant to fire so many missiles and would need to be much more strategic about their targets.

²⁰And they should avoid computers running anything other than a secure OS like Tails, but that'd be another zine entirely.

DEVICE ENCRYPTION

Current iOS and Android devices encrypt your personal data by default using features with names like Data Protection or Full Device Encryption. The strength of this encryption against cracking by police or whoever else gets a hold of your phone is primarily dependent on the complexity of the unlock method (PIN, pattern, or password) and whether the phone uses a dedicated microchip to handle the disk encryption.

On higher-end phones and all modern iPhones, device encryption implementations use a hardware security module (HSM) or a security coprocessor.²¹ These are special microchips in the phone that handle encryption, decryption, and the corresponding cryptographic keys. These chips are important because they protect the keys from unauthorized access and tampering and limit the number of guesses someone can make before the keys are destroyed and the device is permanently undecryptable. These chips may impede adversaries from accessing your data, but it is no guarantee. On lower-end and older phones, no such microchip is used, and the strength of the encryption relies entirely on the strength of your password.

Tools like GrayKey are capable of exploiting bugs in HSMs, and in some case they can quickly crack the unlock password and decrypt the data. The HSMs that may be secure today might have new bugs discovered next month, and law enforcement may develop new techniques for recovering data some 5 or 10 years in the future. A high profile example of an HSM failing to protect data is when the FBI cracked the password of the mass shooter's phone about a year after the 2015 San Bernardino shooting. About 5 years after that, it was revealed access to the data was done via a series of exploits against the software in the HSM.

In short, the more truly random your unlock method is, the more guesses it will take before your data can be decrypted, and a HSM limits the total number of guesses to something very small. Though, even with a HSM, ensure you're using a strong unlock method. A 10-digit or 10-point pattern is guessable within a day on current hardware. In comparison, four randomly chosen words would take over 800 years to guess. This method — called Diceware — is discussed later in this zine.

The use of device encryption may help protect against data capture, but **the only way to ensure that data does not get into law enforcement's hands is if that data never existed in the first place.**

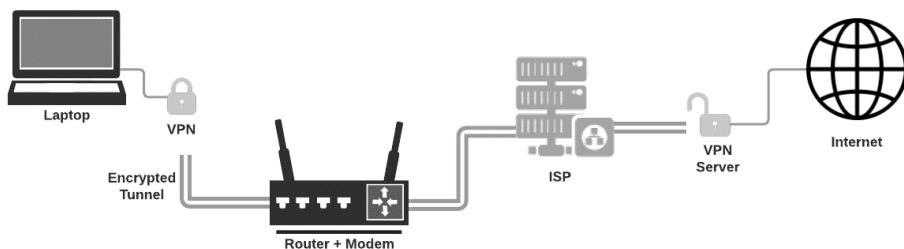
VPNS AND TOR

A virtual private network (VPN), in the context most activists use the term, refers to an application that securely routes all of a device's internet traffic to a service that forwards the traffic to its intended destinations. This might be the person running your café's WiFi, the ISP, or the government. VPN connections are frequently called

²¹This microchip is called the Secure Enclave on Apple devices and Titan M on Google devices.

“tunnels” because of how they provide an encrypted channel from the user’s device to the service. This tunnel protects the traffic from both observation and tampering, but only from your device to the VPN provider. The traffic from the VPN provider to its destination only has the same security guarantees as if it was sent from your device itself.

The main benefit of VPN use is that they prevent every piece of hardware and anyone watching the connection from seeing (most) metadata or content. This can prevent law enforcement from passively observing your traffic or requesting it from your ISP. It can prevent hackers who are on the same WiFi network as you from tampering with your traffic and the router software itself from tracking what sites you’re visiting. This is of particular interest to us as targets of State surveillance because tampering with web traffic is a common malware installation method.



VPNs should not be relied on for anonymity. For that, Tor — and specifically Tor Browser — offers stronger guarantees. A simplified explanation is that Tor Browser routes its web traffic through a series of VPNs chained together where no single device in the chain knows both the source and destination of the traffic. Because of limitation imposed by the OS, Tor Browser is not available for iOS.

Where most VPN software is set up to tunnel *all* of your devices traffic through its service, Tor Browser only affects its own web traffic.

VPNs can leak traffic if used incorrectly. They can be legally compelled to collect logs. If the source and destination of traffic are in the same jurisdiction, law enforcement could correlate the traffic (easier with a VPN, harder with Tor). For this reason, the VPN server or Tor exit node should be outside the jurisdiction of the region you reside in.

Also, the security or privacy properties attained by using VPNs are overstated by their marketing departments and their most fervent proponents. Security and privacy properties require a large amount of trust in VPN providers to do what they claim to be doing, be technically skilled enough to have a minimal chance of being hacked, and resist requests made by the State.²² Reputable privacy-focused VPN providers are generally trustworthy.

²²For example, Mullvad, long the most recommended by radicals, recently drew ire because their founder and co-owner Daniel Berntsson is the primary funder of the fascistic third-positionist Örebropartiet. Fuck 'em forever.

In short, VPNs provide some security but only provide slight anonymity in a few cases. Tor and Tor Browser provide with both security and anonymity. VPNs and Tor should be used when possible.

IMSI CATCHERS

An IMSI catcher²³ is a device that spoofs being a legitimate cell tower and induces phones to connect to it. Once connected, the IMSI catcher can eavesdrop on SMS messages or phone calls as well as inject both of them. They can also collect metadata about web traffic and even tamper with plain HTTP traffic. In some regions they may be deployed without a warrant for the purposes of mass surveillance, in particular during demos to mass collect a list of devices and subscribers who are present. There is also reasonable speculation that they are commonly used as part of covert targeted surveillance operations. Some forms of IMSI catchers are detectable, but the absence of detection does not mean that it is not happening.

In part, IMSI catchers work by downgrading a phone's communication protocol to one with no or ineffective encryption. Even though smart phones have preferences for protocols that offer more protection against interception and spoofing, to enable phones to function in regions with only 2G, and because it is part of the GSM standard, smart phones can still be downgraded into using insecure protocols by IMSI catchers. Phone calls and SMS messages sent and received by smart phones are as vulnerable to interception by IMSI catchers as calls and SMS messages sent and received by simple phones.



FARADAY BAGS

Phones send and receive information using electromagnetic waves. These waves can be blocked by conductive materials. Urban legends and some supporting evidence say that signals can be blocked by putting a phone in several crisp bags that have foil lining, but this — like many countermeasures — should not be relied on. A purpose-built Faraday bag can be acquired, and these can be counted on to block all phone

²³They are often referred to by the popular brand name StingRay.

signals when used correctly.

When phones are powered off, they may go into a low-power mode if you enabled a feature or app like Apple’s Find My (for locating phones and other devices). This feature will periodically send and receive signals so that your phone is locatable. Also, malware can hijack the shutdown routine and prevent the phone from actually powering off when you try to shut it down so that it can continue to report your location. If you have not enabled apps or features for finding a lost/stolen phone, and if your phone is not infected with malware, then when you power it off, it will not be locatable.

However, you may want to use a Faraday bag to prevent your phone when powered on from being locatable by being able to connect to cell networks, WiFi, or Bluetooth devices.

SECURITY BASICS

There are some practices that tend to be advisable for most activists (or most anyone for that matter). A few are detailed here.²⁴

UPDATES

Without reservation, the single best thing you can do to prevent yourself from getting hacked by law enforcement — or random hackers — is to promptly install updates to your phone’s operating system and all apps as soon as they become available. It may be annoying, but many updates contain security patches for critical vulnerabilities.

PASSWORD MANAGERS

The second most useful and generally applicable security practice is to use a password manager for all your accounts, including those used on your phone. There are paid versions that allow automatic synchronization of passwords across devices and automatic logins to web-pages. However, these require some level of trust in the corporation offering the product. Free alternatives like KeePassDX exist but do not have the ease of use that paid products do.²⁵ No matter if you use a digital password manager or a notebook, all your accounts should have strong, unique, random passwords. These can be automatically generated by the manager. The master password to unlock the manager as well as your phone should be long, random phrases.

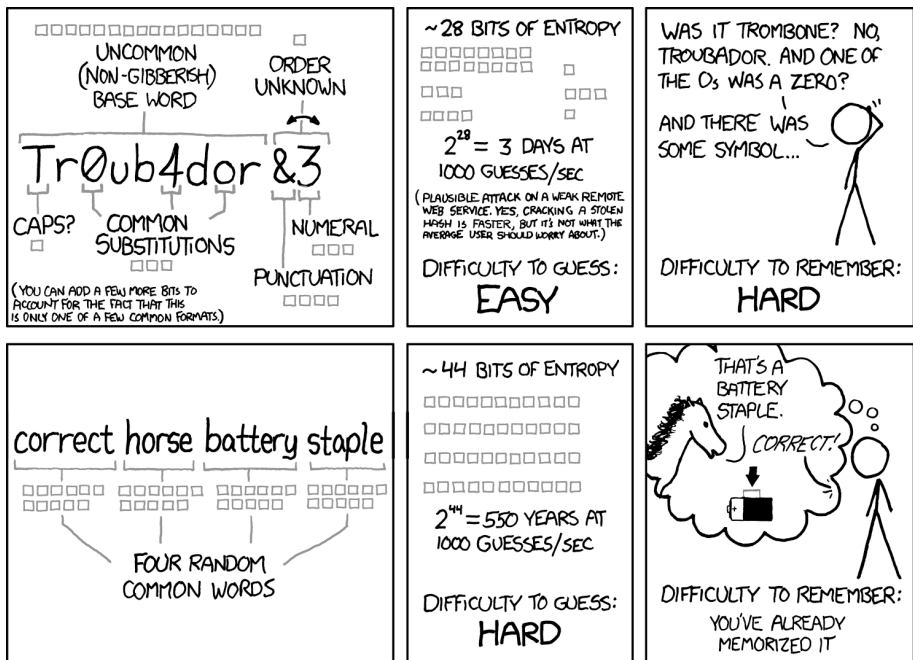
Numbers	Word
24311	drowsily
24312	drudge
24313	drum
24314	dry
24315	dubbed
24316	dubiously
24321	duchess
24322	duckbill

²⁴Please also note that some of these apply to using computers too.

²⁵In all cases, but especially with free open-source tools, it is critical to regularly make backups.

Humans are notoriously bad at generating the randomness needed for passwords, and using the opening line of your favorite poem, or some tricky substitution rules to change *antifascism* to *an7if4sc1sm!* are no challenge for a motivated individual, and they can be quite easily cracked by computers. Diceware is a method of creating passwords by rolling dice and using them to select words from a predefined list. Four words is the absolute minimum, six is better, but anything over eight is overkill. Doing this provides unguessable randomness that human brains cannot create on their own, and moreover this randomness is easily memorizeable. An English-language, user-friendly wordlist is provided by the EFF.²⁶

XKCD 936 — “Password Strength” — 2011.08.10



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

LOCKING YOUR PHONE

Depending on your threat model, you may want to make it difficult or near impossible to unlock your phone. This is of particular importance because the unlock method

²⁶The original list has many difficult to memorize “words” like *aaaa* and *jk1*. Use eff.org/dice instead.

ties into the decryption method, so a strong unlock method helps defend against unwanted access to your data if your phone is captured. In general, passwords are preferable to both PINs and patterns as the former are harder for machines to crack. You should almost certainly disable face-unlock features, and you may want to disable fingerprint unlock too. In some regions there are legal protections for passwords but not for fingerprints or other biometrics, and you can be legally compelled to unlock a phone with your finger but not with a password.

Some phones offer the ability to have all data deleted if there are too many incorrect login attempts. You should enable this (and then keep your phone away from curious toddlers and pets).

Disable notification content from appearing on your lock screen, or at least disable them from apps that might have sensitive information. Disable access to apps from your lock screen.

If you have device encryption enabled on your phone, your data is most strongly protected when your phone is off (or has been powered on but not unlocked yet). After unlocking your phone once, you have less strong protection for your data.

Many activists leave fingerprint unlock enabled because it is tremendously convenient compared to typing a 30-something character password 100 times per day. Because the need for convenience often wins out over the need for better security, this becomes yet another reason to not keep sensitive information on your phone. If you have fingerprint unlock enabled, you can temporarily disable it by holding down your power button, possibly also tapping a “Lock” button after. You can do this before interactions with law enforcement, going to bed, or leaving your phone unattended. Make sure you test this before you have to rely on it.

Some OSes (including GrapheneOS) offer a duress password or PIN. If this is entered, it will perform an uninterruptible factory reset in the background. This may be worth enabling, but also note that entering this could land you with a charge of destroying evidence or interfering with an investigation.²⁷ Know the risks in your region before enabling this feature. A method that might get around the legality of this would be to keep a note labeled “Password” with your duress password clearly written on it in your wallet and on your desk. A cop might think to enter this which would wipe your device. In this case, they would have destroyed evidence, not you.

Further, GrapheneOS offers a feature to have the phone automatically reboot after a set period between unlocks. It is enabled by default on an 18-hour timer. This helps protect your data if your phone is seized but in an unlocked state and your adversary delays on attempting to access it.

²⁷“Concern over US effort to prosecute Sam Tunick, accused by authorities of wiping his phone using GrapheneOS” from “US government targets Cop City protester over phone operating system” published by *The Guardian*. <https://www.theguardian.com/us-news/2026/jul/23/cop-city-protester-phone>.

Related, see “Cada vez que vemos un Pixel pensamos que puede ser un narcotraficante”. La policía apunta al móvil de Google como el favorito del crimen” in *Xataka*. <https://www.xatakandroid.com/sociedad/cada-vez-que-vemos-google-pixel-pensamos-que-puede-ser-narcotraficante-movil-perfecto-par-a-crimen-sencilla-razon>.

LOCKING DOWN YOUR PHONE (AND ACCOUNTS)

Google and Apple both offer features for individuals and organizations that might be targeted by sophisticated adversaries such as States, state-sponsored hacker groups, or corporations doing espionage. For Apple accounts and devices, this feature is called Lockdown Mode. For Google, this is called Advanced Protection. These features have some trade-offs. They might break some apps by disabling features known to be exploited by malware. Advanced Protection disables installing apps from F-Droid or other third party app stores, thus locking you more into their closed ecosystems. If you are using iOS or a stock Android OS, you should consider enabling the applicable feature.

WIRELESS FEATURES

You may want to disable WiFi, Bluetooth, and/or your mobile network when you are not using them. These can be used for “fingerprinting” and uniquely identifying your phone. Additionally, they increase the number of ways adversaries might try to break in to your phone. While the risks from leaving them continuously enabled are low, these practices can improve to your security (and increase your battery life), so if you don’t need them, why not do this?

BACKUPS

Smart phones often come with a feature for automatic backups to a cloud account tied to the phone (to Apple for iOS and to Google for Android). Both Apple and Google offer end-to-end encrypted backups that, following external reviews, offer strong assurances of privacy from both the company itself and law enforcement. However, these are guarantees are only as strong as the trust in the services to not modify their hardware and software at the compulsion of the State.²⁸

Additionally, some apps may have their own backup services. For example, WhatsApp and Signal can both backup your conversations to their respective servers.

Our recommendations are to avoid backups to corporate servers when there is any data on your phone tied to your activism. Backups of Signal conversations are considered sufficiently safe at this time. You should consider periodically backing up your data to an encrypted hard drive or encrypted USB stick that you keep somewhere safe.

²⁸The UK government is still trying to compel Apple to grant police privileged access to encrypted backups. “Apple launches legal challenge against UK government demand to access data.” *The Guardian*. 2026. <https://www.theguardian.com/technology/2026/aug/03/apple-legal-challenge-uk-government-data-access>.

CHAT APPS

Chat apps provide more secure and more feature-rich alternatives to telephone calls and SMS messages.

ENCRYPTION

Text and voice chat apps offer one of two types of encryption.

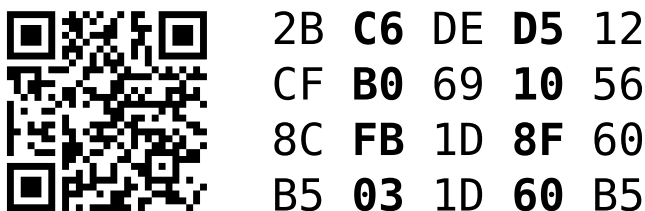
Client-server encryption is when the channel between a client (e.g., an app) and the server is encrypted and protected from interception or tampering. The message is decrypted, processed, and/or stored on the server. When the message is requested by another client (e.g., your friend's phone), it is re-encrypted for transit and sent.

End-to-end encryption (E2EE) is when clients generate cryptographic keys and exchange their public parts with each other. Messages are encrypted using the other client's public key and sent through the server (or servers) with the server only acting as a blind relay because the messages are only decryptable by the intended recipient.

E2EE only means that a server or someone else between your phone and your comrade's phone cannot read or tamper with a message. An adversary may infer information from the message's metadata such the size of the message, the time it was sent, its sender, and its recipients.

Some messenger apps offer optional E2EE such as Telegram with their "secret" chats, but this feature is not available for groups. Other apps have mandatory E2EE such as Signal, iMessage (Apple), and WhatsApp.²⁹ Some apps like Element/Matrix have E2EE enabled by default, but it can be disabled for compatibility with older clients.

QR Code and Fingerprint



The security of E2EE depends on the verification of the exchanged keys which is often done by scanning QR codes containing a fingerprint that is unique to the generated key. Some apps require you to only verify one fingerprint for all devices,

²⁹There are more interesting peer-to-peer chat apps like Cwtch, Delta Chat, and (now in maintenance mode) Briar that are metadata resistant and possess other interesting security properties, but they do not have wide adoption.

while others ask you to verify one fingerprint for every app or device. Some apps send notifications in the conversation notifying you when your contact's fingerprint changes, possibly suggesting something nefarious, though more often than not it just means that the app was re-installed on the existing phone or installed on a new phone. Some apps unfortunately do not provide such warnings. You **must verify** all fingerprints for all devices, and if a fingerprint changes, **you must re-verify it** otherwise the security offered by the apps could be undone. Further, some chat apps do not share devices you've verified with your other devices, and this poor UX requires you to verify each of your contacts' devices from each of your own devices.

If this sounds confusing, it is because it unfortunately is, often in many ways. For example, the QR code you use to share your Signal contact with someone is not the same as the QR code used to verify the fingerprint of your contact's keys. You have to scan both! In two separate steps!

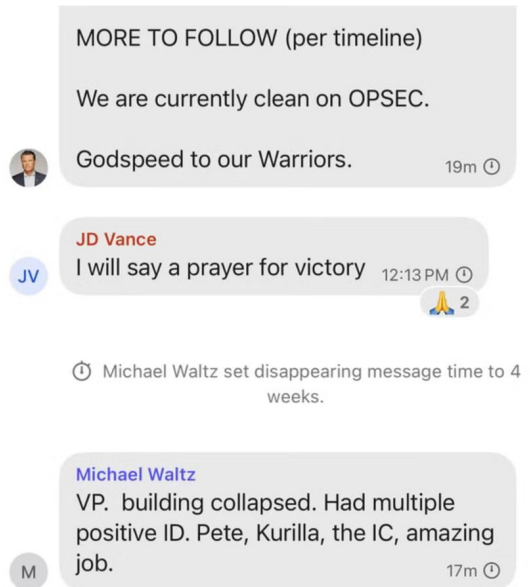
USAGE

The mantra "Just use Signal" is often repeated by activists, and while it generally is a very good app, this mantra falsely assumes that everyone has identical threat models. In some regions, use of Signal may be blocked by national firewalls, or its use may be so infrequent that it could flag a user as suspicious. In North America and Europe, these drawbacks generally do not exist. Another common complaint against Signal are that contact lists are shared with the server in merely semi-secure ways to allow for contact discovery and initial key exchange.³⁰ Also, that it has central servers *at all*.

For most apps, when messages are received, they are decrypted and stored in plaintext on the device, which is fine as long as the device has full disk encryption and does not become infected with malware.

Some apps like Signal allow you to set a password to prevent access to the message

³⁰ A previous complain was that it requires phone numbers, and while this is still the default method, it is possible to do without. <https://support.signal.org/hc/en-us/articles/11197884108826-Phone-Numberless-Registration-for-Android>



Someone in a Signal chat of high-ranking US government officials accidentally added the editor-in-chief of *The Atlantic* to the group as they were discussing imminent military strikes against Houthis in Yemen. Contrary to what the US Secretary of Defense thought, they were not "clean on OPSEC." Don't be like these fascist chucklefucks.

while someone else is using your phone, but this does not re-encrypt messages or attachments in any way.

Because messages are stored in plaintext, and because they might be recoverable even with device encryption, you may want to enable disappearing messages. On some apps, one party may enable disappearing messages for everyone in the chat. On other apps, each party must enable disappearing messages to ensure all messages eventually disappear. It may be inconvenient to have disappearing messages as searching for an image, file, or some decision is only possible as far back as say 1 week or 1 month. This may be preferable to having a multi-year long log of everything you've said or thought, and in particular everywhere you said you've been.

DON'T “JUST USE SIGNAL”

Various privacy orgs and concerned activists did an excellent job encouraging the adoption of Signal in the wider public and especially among activists. They did possibly *too* good a job as many individuals took this to mean “If you use Signal, then you are totally secure.” This has led to some people discussing things they absolutely should not discuss over electronic mediums and then assuming it's fine because they used Signal. Every security countermeasure has some set of assumptions it works with, and from that there may be accepted risk or things that are out of scope. Signal is very good at preventing a State-level actor from using mass surveillance to read the contents of text messages. It even hides some — but not all — metadata. Other chat apps have roughly a similar threat model. However, if your phone is compromised by malware because you have drawn attention to yourself or simply gotten unlucky, Signal will not prevent your communications from being read.³¹

Before any app can encrypt a text, it needs to get it somehow. The virtual keyboard used for this is also an app. This makes it especially critical as it interacts with *all* the text you enter into your phone.

For some languages, in particular languages based on characters rather than letters, an Input Method Editor (IME) is used to convert sequences of Latin letters into the target language's characters. These are often third-party apps that are (pre-)installed. Signal fails to adequately warn users who use IMEs about the possibility that their chats could be read by the software and reported to the State before the messages were encrypted.

Signal is not a guarantee of safety. The same goes for any other E2EE chat app. Do not treat them as one.

While we have strong criticism for Signal here, it comes from a place of appreciation, and it is primarily driven by Signal's popularity and the misconceptions around it. It is still at the time of this writing one of a small number of encrypted chat apps that can be relied on for strong security.

³¹Further, some folx have atrocious security practices of joining many large Signal group chats and discussing their actions without vetting who else is in the group. It doesn't matter how good the encryption is if one of the group members is an infiltrator or snitch.

Input Method Editor and Pinyin Candidates



There are many flashy news stories, social media posts, and (ironically) Signal chain messages about how Signal “has been hacked” or “is fundamentally flawed.” Most of these are bullshit fear mongering so that the poster or journalist can get attention, or the person making these claims truly has no idea what they’re talking about.

Has Signal been hacked?

No.

hassignalbeenhacked.info

All that said, Signal is critical anarchist and activist infrastructure, and even temporarily blocking it at the network level during a series of raids could have devastating effects for our movements. We should all keep this in mind and plan around it.

OTHER COMMON CHAT APPS

As mentioned before, iMessage and WhatsApp offer E2EE, and both use the Signal Protocol. Facebook Messenger also uses this protocol for secret chats as did Microsoft Skype for private chats. These apps may be preferable to unencrypted SMS in some regions where Signal is blocked, but this depends on the ever-shifting whims of the corporations and the extent to which they mine message content pre-encryption for advertising purposes.

Because of their marketing, Telegram has undeservedly earned a name as an encrypted chat app. It is not. Telegram has opt-in E2E encryption for one-on-one chats,

but not group chats. Its code has been described as containing “the most backdoor-looking bug I’ve ever seen” by a cryptography expert,³² and it has over a decade of devastating critique of its protocol and cryptography. More worrying, it’s extremely suspicious that a network engineer at Telegram has companies with contracts with the FSB, a Russian state security agency.³³ Its protocol also poorly protects metadata about who is messaging whom. Activists should not use Telegram, unless — like it was mentioned above — there truly are no functioning alternatives. If you do, be aware of who might be listening and mapping your social network.

E-MAIL



GnuPG? More like Gnu Pain Generator, amirite?

There are ways to make e-mail communication more secure, but e-mail as a protocol and communications medium is generally not secure for private communications. When sending e-mails, some people use PGP³⁴ but this is difficult to use and has an overall poor user experience. Two people using these encryption methods can have fairly good protection against having their e-mail read, but one misclick can send the entire history of a conversation in plaintext thus making it subject to dragnet surveillance and viewable by law enforcement. ProtonMail has made bold claims about encryption for their e-mails and clients, and many activists have taken these misleading statements to mean that using a ProtonMail account means *all* of their e-mails are encrypted, but this is not the case.³⁵ E-mail should generally be avoided for planning and especially for secure communication.

That said, e-mail remains popular because every device can send and receive e-mail, and some people “don’t do chat apps.” For coordinating a local tenants’ union or setting up shifts at the local infoshop, e-mail may be fine. If you choose to use e-mail, assume that law enforcement are reading all messages, and keep conversation to a minimum. Do not discuss illegal activities. Do not discuss juicy scene drama

³²“The Most Backdoor-Looking Bug I’ve Ever Seen” (2021), <https://words.filippo.io/telegram-ecdh/>.

³³“Telegram, the FSB, and the Man in the Middle” (2025), <https://www.occrp.org/en/investigati-on/telegram-the-fsb-and-the-man-in-the-middle>. “Журналисты и правозащитники обвиняют Telegram в связях с ФСБ и раскрытии данных пользователей. В мессенджере теперь и правда опасно общаться?”, <https://meduza.io/feature/2025/06/11/zhurnalisty-i-pravozaschitniki-obvinyayut-t-elegram-v-svyazyah-s-fsb-i-raskrytii-dannyh-polzovateley-v-messendzhere-teper-i-pravda-opasno-o-bshatsya>.

³⁴Pretty Good Privacy, software that encrypts and signs files using the OpenPGP standard. People use the software GnuPG (Gnu Privacy Guard, also called GPG) to handle encryption. Yes, these naming conventions are confusing nerd shit too.

³⁵ProtonMail can also eat shit because of their cooperation with law enforcement, their censorship of accounts, and their CEO Andy Yen praising the US Republican Party. This isn’t saying never use them, just that... well... It’s not easy to find reliable e-mail services that also care about privacy, so at least be aware of what you’re getting into if you do.

that can be exploited by the State.

Finally, there are legitimate use cases where e-mail and PGP can be a last resort such as a one-time-use encrypted channel for someone on the run so that they can set up a second more secure channel.³⁶ In cases like this, phones should still be avoided because of their ease of trackability.

SUPPLY CHAINS AND TRUST

We rely on supply chains in every aspect of our lives: the delivery of clean water, the removal of waste water, the delivery of electric power, the delivery of food, and so on. Despite privatization of essential resources and capitalistic (or otherwise authoritarian) incentives to deliver the lowest quality version for the most profit, these supply chains generally are able to regularly and safely deliver us the goods and services we need.³⁷ Some of this is regulation, some is to protect reputation and thereby profit, and some is that organizations are not homogeneous and that individuals at them want to still help others meet their needs.

The supply chains related to digital technology in comparison to physical goods are susceptible to more targeted interference that's less detectable, and this tends to rouse paranoia. However, these supply chains still tend to still be resilient against interference because of companies protecting their reputation (profit) and the risks if a foreign entity takes advantage of hidden backdoors. Some people like to make bombastic claims about the safety of digital tech supply chains, sometimes ones that are or were technically true like "Tor is funded by the US State Department." These are as much red herrings as calling out a comrade for "having been paid by the State" because they were once a janitor at a public school.

More concretely, in order to trust that an E2E encrypted message sent by your phone to another both arrives and can only be read by the recipient, one has to trust all of the following:

1. The microchips on the phone do not have backdoors.
2. The OS has no backdoors in the source code.
3. The version of the OS installed matches the source code.
4. The apps' developers have not built backdoors.
5. The version of the apps installed match the source code.
6. The cryptographic protocols used were not designed with secretly breakable maths.
7. And so on...

³⁶For a short story that covers this, see *Survival* on CrimethInc. and the linked article *An Anarchist's Guide To GPG* on C4SS.

³⁷Look, they're not *ethical*, and there are plenty of counterexamples of unsafe and inadequate supply chains, but that we in Rich World nations are mostly able to get food, water, power, and waste related needs met despite all the fuckery is still kinda impressive.

The good news is that there are ways to make verifiable builds of OSe and apps, and that nerds are pretty decent at finding traces of tampering and then reporting on them. The bad news is that this landscape is constantly shifting, and one must pay attention to the news and gossip to make sense of who or what can be trusted and to what extent.

What further complicates this is that many of the individuals in the world of digital rights, anti-surveillance, and privacy come out of the cypherpunk tradition which, much as it has a left-anarchist leaning, it has a right-libertarian wing as well. There are crypto-fascists aplenty — crypto both in the sense of hidden and them being obsessed with cryptocurrencies. Brendan Eich was briefly CEO of Mozilla (the company/foundation developing Firefox) and is currently the CEO of Brave, a company that makes the allegedly privacy-oriented web browser of the same name. He, among other things, has made political donations against same-sex marriage and peddled COVID-19 conspiracies. Major figures associated with Mullvad (the VPN provider) and Proton (the VPN and e-mail provider) have been likewise mentioned elsewhere in this zine as being our ideological nemeses.³⁸ The list of authoritarians, “free speech” libertarians, fascists, rapists, etc. within the privacy and security space is higher than one might expect.

To summarize this: the technical foundation on which much of our phones and their apps are built are not as solid and ideologically aligned as we might hope, and it’s possible we reach a point where we actually have to abandon them. But luckily we’re not there yet, and may never be.

MULTIPLE ALIASES, MULTIPLE PHONES

Depending on your threat model, you may choose to maintain multiple phones that are linked to your multiple aliases. For example, you may have one phone linked to your status quo public life with social media accounts you use to connect with family and a second phone with a separate SIM and separate accounts tied to your activist life. This segregation of accounts is part of a process called compartmentalization.

The first benefit is that the use of distinct devices for each of your aliases prevents apps or user errors (e.g., accidentally pasting something) from exposing your private information in the wrong context. Apps on your phone may have unexpected behavior such as sending your entire contact list a request to connect when you sign in to a new messenger app.³⁹ You may make a mistake and reply to a social media post from the wrong account. When you click on an e-mail address intending to use one of your aliases, your phone’s OS might start composing an e-mail with a default e-mail client tied to a different alias.

The second benefit is that your activist device can be minimal and only used for secure communications. Each app you install is a possible route for malware to get

³⁸Check the footnotes.

³⁹Yes, a real example from a (now abandoned but still technically functioning) privacy focused app.

on your phone, so if your phone has only a bare-bones OS and two chat apps, it is more difficult to compromise.

Using multiple phones on its own does not prevent law enforcement from tying your aliases together. If you carry the phones at the same time or use them at the same locations, they can be linked.

As an alternative to multiple phones, you can reduce some of the risk of leaking data via error or unexpected behavior by creating multiple profiles on your Android device. This will not protect you against malware, but it does offer some protection against information leaks.

One of the most common use cases for having multiple phones is for organizing a union. Some companies require apps to be installed for remote management as a way to protect corporate intellectual property or to mitigate security breaches.⁴⁰ These are spyware apps in fancy clothes, and they can completely control your phone. Even those aside, many companies require a chat app for communicating. You should avoid organizing on company devices or ones with corporate spyware installed, and you should avoid using company chat in unionization efforts.

DISPOSABLE, DEMO, AND BURNER PHONES

Most people understand the importance of their phones and know that they can be tracked by them or that their compromise or loss can be devastating. A number of approaches are used by activists to help reduce their risk even if they cannot fully articulate this risk or why such countermeasures work.

Some people have demo phones or disposable phones they take to actions or use when crossing borders. These devices have minimal private data on them and are considered untrusted — due to possible malware installation — if they are handled by law enforcement. These phones are not used for anonymity. They may share a SIM card with their user's everyday phone and may be used in such a way that geolocation would link them back to their user's residence. Demo phones make less data and less accounts available to the police should they be captured. There is no requirement that a demo or disposable phone be a simple phone. In many cases they are smart phones because this allows their users to connect to public WiFi, have (offline) maps, and to have and E2EE communications.

Activists erroneously use the phrase “burner phone” to describe demo phones, disposable phones, or any simple phone.⁴¹ A burner phone takes its name from the fact that it is single use and after that it is destroyed, or a factory reset is performed and then they donated to somewhere geographically far from where it was used. They are acquired when the user needs to have mobile communications during the sort of action that will lead to a massive and concerted investigative response.

⁴⁰If your company requires it, demand they give you a work phone. Also, join your local union to ensure these demands are met and your rights as worker retain some protections.

⁴¹People seem to use the phrase “burner phone” because it sounds Mega Illegalist and Super Crimey and not because they are actually describing the properties of a burner phone.

For a phone to be a burner phone, it needs to meet the following criteria:

1. The phone must be purchased using cash.⁴²
2. The SIM card used for the burner phone must be purchased using cash.
3. The phone and SIM card must be purchased by a person with no other phones or traceable devices on their person at that time.
4. The phone and SIM card pair must only be used with each other.
5. The phone must never be taken to locations associated with the user unless it is both off and in a Faraday bag.
6. The phone must never be used in the presence of non-burner phones or other devices that can be tracked back to the user or their associates.
7. Any accounts on the phone must be made anonymously, only ever used with that phone, and then never used again.
8. The phone must be used for exactly one action.
9. The phone must only ever contact other burner phones or unaffiliated parties (e.g., an office or adversary who is targeted by the action).
10. The phone must be powered off after the action then immediately destroyed or reset and donated. The SIM card must be destroyed.

A complicating factor is that some phones or SIM cards require activation either by calling a number or accessing the provider's website. Sometimes these websites block Tor connections. Using a non-burner phone to activate the SIM is an obvious violation of their required security properties. You may need to find a pay phone or socially engineer a stranger at a train station to let you borrow theirs for just a few minutes.

A further complication is the legal requirement in many regions for a SIM card to be tied to a valid identification document before activation is possible.

When we say that a burner can be used for one action, this means both an action that takes place over only over a few hours as well as the planning and coordination in the month before the action.

With particularly careful usage, a single closed affinity group can reuse their set of burner phones for recurring actions. If this is the case, the phones need to be cycled in batches so that the different closed loops of burners don't overlap with each other.

A non-mandatory, but strongly recommended property is that burner phones should not be purchased immediately before an action. This extra time increases the chances that the stored security footage of the purchase would be overwritten or exceed the maximum retention period.

Attempting to obfuscate the existence of the closed loop between the phones can help prevent the detection of the affinity group. One step is not activating them all

⁴²Theft of phones with an activated SIM card is generally not recommended because each theft creates an additional location data point that can be tied to the action and reported to the police, the phones might not be able to be unlocked, and the owners may have the devices added to deny-lists maintained by the carriers so that they cannot be used for connecting to mobile networks.

in a short time frame. Gradual activation is less detectable when the State analyzes the data. Make a few phone calls from random locations to numbers someone would plausibly call, but **do not** speak if someone picks up. Call numbers with expected long wait times like banks or insurance companies. Call a few local shops before they open or after they close. The fake phone calls may be unnecessary as many users in certain regions never place phone calls and simply use their data plan for everything.

Because of the carefulness with which a burner must be acquired and used, it is highly unlikely that it is worth the trouble. If you think your action requires a burner phone, you should almost certainly attempt to find a way to do the action without any phones at all. To help make it clear to others that a burner phone must have these properties, avoid use of the phrase burner phone and prefer demo or disposable phone when applicable.

TURN IT OFF? LEAVE IT ON?

A topic of considerable debate is whether for meetings or actions if phones should be brought and left on, brought to meetings and turned off, or left on at one's home or somewhere else safe. The debate rages because of logistical considerations, the security properties each option offers, and convenience versus assumed security being weighed against each other.

One of the goals of counter-surveillance is to become uninteresting so that algorithmic surveillance doesn't flag you or so that humans looking at data don't take note. Something that is rather interesting is when phones are powered off, especially if many phones that are near each other or if phones regularly go off at the same time such as every Monday at 18:15 (to account for the 45 minutes of travel to a 19:00 meeting). A phone that is powered on, is in a locked state, and left at home runs a slightly increased risk of seizure by an adversary, but it creates no interesting data.

If you choose to power off your phone to hide your movements and associations, you should additionally randomly power it off on different days at different times so that someone looking at historic data cannot say for certain that every time your phone is powered off that you are doing something "interesting."

If phone are needed for meetings for whatever logistical reasons, we suggest using something we will call the Café Chatter Method to reduce the likelihood useful information can be recorded by the phones. The method has the following steps.

1. A soundproof — or at least sound-dampening — container is obtained.
2. A separate room is designated as the phone storage room.
3. The first person to arrive uses their phone to play a background soundtrack of "café chatter" — ideally downloaded for offline use — on a loop at high volume from the phone's main speaker. They put their phone in the container, and they put their container in the storage room.

4. When each person arrives, existing conversations stop. The new arrival leaves their phone on, optionally plays their own “café chatter” soundtrack, and adds their phone to the container.
5. The meeting resumes.
6. When someone leaves, conversations stop until the person has retrieved their phone and left earshot.

This is not foolproof as skilled audio engineers could isolate the real conversation from the fake conversations playing from the phones. It is, however, a barrier that may make it impossible to recover actual conversations, and at a minimum it increases the effort an adversary must use to get the conversation’s content. This increased effort could exceed your adversary’s time, skill, or budget and therefore prevent intel from being gathered. Likewise, it does not inhibit physical surveillance methods, but still, it increases the costs of surveillance.

Another option is for attendees to power their phones off before travelling to the meeting and place them in Faraday bags. This creates some variation on when they power off thus making correlation harder, and it doesn’t reveal the location of the meeting. It is still somewhat suspicious, and it is unclear if this creates more risk than bringing phones and using the Café Chatter Method.

Our recommendation is for phones to be either left on, locked, and at home. Second best is to use the Café Chatter Method.

GRACEFUL DEGRADATION

This zine principally discusses ideal characteristics for secure phone usage, but often these ideals are not attainable. One such example is if you are organizing with people who cannot afford smart phones. Getting cheap simple phones to a network for organizing an action or even for coordinating regular meetings can be easier and more financially manageable than doing the same with smart phones. Unfortunately, the lack of encrypted voice and chat apps means increased surveillance for your messages.

To prevent the State from gaining too much information about your actions, you will have to rely on human solutions rather than technical solutions. An agreement to only ever discuss meeting times and locations with a minimal amount of information can reduce the gathered information to an absolute minimum. A simple codebook that replaces common phrases used in organizing with random, innocuous code phrases can create misdirection if someone attempts to investigate, and the use of code phrases can prevent automated systems from alerting authorities.

Using patterns like this allows you to gracefully degrade from higher security to lower security without completely exposing yourself to surveillance and State repression. These methods require greater care and effort, but they are doable.

MAKING A PLAN

We cannot pretend to know your threat model, and we cannot address every bit of nuance for every region and situation. What we can do is list some guidelines that are generally applicable. When reading these, you need to consider what is practical. What can you actually do? And what will people in your social circle do? Your new plan doesn't have to be perfect. It just has to be better than whatever you're doing now. If this means making compromises on security so you can continue to organize, you may have to do that. But at the same time, don't let others' poor security endanger you. Find a balance, but also set boundaries.

The following is by no means an exhaustive list, but these are some ways to develop personal operational security and group security culture:

- Use a smart phone as they are more secure against most threats activists face than simple phones.
- Do not bring your phone to activities that might interest police, and in particular protests that might be rowdy.
- Prefer E2E encrypted apps for communication, enable disappearing messages, and avoid e-mail.
- Use a password to unlock your phone, and enable device encryption.
- Disable fingerprint unlock on your phone before going to bed or leaving it unattended.
- Regularly back up photos and other data to an encrypted drive and remove them from your phone.
- Delete old data: DMs, group chat, e-mails, calendar events, etc.
- Leave group chats where you do not need to be present, and remove inactive members from group chats.
- Practice leaving your phone at home or powering it off when running errands or for small actions to habituate yourself to its absence.
- Ideally, conduct meetings without phone let on and at home. Next best is to use the previously discussed Café Chatter Method of placing phones in a sound-dampening container, playing an ambient chatter recording, and putting them in another room.

And most importantly:

Do not send messages or make voice calls about highly sensitive matters. Do not photograph or film incriminating things. Do not create evidence that can be used against you or others.

VOID WHERE PROHIBITED

What was written here, and even the rest of this zine, are guidelines. They may not apply to you. In particular, digital security can leave particularly noticeable trails. If Signal is very uncommon in your region, its use could make you a target. VPNs may be criminalized. Use of Tor may get you a visit from the police. The presence of secure communication apps on your phone could turn your arrest into a disappearance. Before you download anything, do research about repression in your region to determine if the guidelines we have provided will make you safer or if they will endanger you.

ALTERNATIVES

It is always easier to say “do this instead” rather than “don’t do that,” and when trying to change behavior or practices, providing alternatives increases the chances that someone will drop the old, insecure behavior. There are legitimate reasons to have phones, and alternatives can mean less burden when we give up our phones or change our habits.

Barriers to getting rid of phones are that people want to communicate easily, have info accessible, gather and record new info, and quickly trade contact details. A pen, a note pad, and a photocopier let you have your collective’s meeting minutes accessible to all in a much less traceable manner. You can use it to trade contact info, and if you’re slick, you can carry a copy of your device’s cryptographic fingerprint to establish a secure line even when you and the other party do not have your phones on you. A paper calendar can allow you to schedule. Printing out paper maps of the area of operations for an action can help you navigate. If you create paper copies of information, ensure you promptly and securely dispose of it after use to avoid creating a literal paper trail of your activities.

PHONELESS CONTINGENCIES

While your plan may work today, you must also be forward thinking. You may rely heavily on your phone for organizing while accepting the security risks, but there may come a time when repression or catastrophe disables your phones or the internet. It is common during heightened repression for the State to cut mobile phone service or the internet for entire regions. If your ability to organize and your safety relies on nearly everyone having phones and working internet, you are setting yourself up for certain modes of failure. Word of mouth and the so-called sneakernet should be incorporated into your planning in case they become the only possibilities for moving information.

CASE STUDIES

To make the previous discussions more concrete, we're providing a number of case studies drawn from our experiences. Some of these cases show individuals who already have thought-out threat models, and others who do not. Some are based on urban legends, and others more on verifiable facts or very probable conjectures. Where there are errors, they are discussed.

CASE 1: PLANNING MEETINGS FOR A SEMI-PUBLIC ACTION

SCENARIO

A collective is planning an occupation that will be kept secret until it begins, after which it will be made public via social media. Planning primarily happens at in-person meetings at a local social center.

ASSUMPTIONS

The collective assumes that police are interested in preventing occupations, and the activists may be under surveillance. This surveillance includes, but is not limited to, State-backed malware that could be on the individuals' phones.

COUNTERMEASURES

To prevent the State from using the phones' microphones to record the meeting, phones are powered off, collected, and placed in an adjacent room.

ANALYSIS

It is correct to say that the phones could have been compromised by malware, and it may be correct to say that moving the phones to another room impedes their microphones in recording the conversations. However, there is an assumption about how effective moving the phones out of the room is, and this could be verified by starting a recording, placing the phone in the other room, then having a loud conversation to see how much is understandable when played back. If the voices are remotely recognizable, snippets could likely be recovered with audio editing software.

If the social center is not regularly swept for microphones or other bugs, the conversations may still be recorded. If the group or other groups who frequent the social center are heavily surveilled, laser microphones placed in nearby buildings and pointed at windows could record the conversations.⁴³

⁴³A very rare occurrence, but also — in some cases — not worth the risk of ignoring the possibility.

If individuals are under passive surveillance, the fact that a meeting took place and who attended could still be revealed by the repeated presence of the same group of phones powering off at fixed location on a recurring schedule.

RECOMMENDATIONS

If the group believes they may be prosecuted for conspiracy to commit a crime, they probably want to leave phones at home entirely. If this can't be done, using the Café Chatter Method discussed early in this zine is probably more advantageous than powering the phones off after arriving to the meeting or before departing for it. These advantages can be further minimized by not bringing the same phones to the action itself. As said before, turning phones off after arriving creates too much "interesting" data that may draw additional surveillance.

If high security is desired, the risk from bugging of the room or recording via State actors can be further reduced by meeting at locations that are not affiliated with liberatory movements. If the group wants to meet at a central, known location for convenience, it should be established at the start of the meeting that only the current action (and nothing more illegal) should be discussed.

CASE 2: OVERHEARD CHATTER

SCENARIO

Some members of an affinity group are hanging out in a park to socialize, not to plan an action. Their phones are present and on, but their security culture includes not discussing past actions or trading war stories as these can contain incriminating information.

ASSUMPTIONS

The group has assumed that the police only want to listen to their conversations if they are about past or future illegal activities. They have assumed that their everyday conversations are uninteresting and uninformative.

COUNTERMEASURES

The group has taken no countermeasures against their conversations being overheard.

ANALYSIS

If the group is consciously not discussing plans or past actions, then obviously no microphone can overhear what isn't said aloud. However, planned and carried-out actions aren't the only thing the State is interested in. Gossip, drama, love interests, social ties, and even the dispositions of people and orgs within a milieu toward one

another are valuable intel. This can allow the State to create more accurate social maps. If the State suspects one individual was involved in something they are investigating, and they know the individual had accomplices, using social maps that are constructed from bit of casuals conversation can help them narrow down their list of suspects or reveal the members of an affinity group. Such overheard conversations can give the State insight about who is feeling ostracized and resentful so that they can be targeted to become an informant. Small conflicts can be exploited, and heated emotions can be fanned into roaring disputes.

RECOMMENDATIONS

There is a generational split among activists between those who organized before the widespread use of mobiles phones and those who began organize after the ubiquity of phones. There is a also a further split between those who organized using simple phones before the popularity of smart phones, and those who have always organized in a world where nearly all of their contacts have smart phones. This gap is notable by the ability to make plans on the assumption the other people wouldn't have phones such as fixing locations and times with less spontaneous changes. Additionally, those who organized prior to the adoption of mobile phones have a more acute sense of what it is like for organizing to increasingly take place where everyone effectively has microphones present.

As mentioned earlier in this zine, smart phones allow us to instantly communicate and have limitless information on hand at all times. This comes with the cost of new avenues for surveillance. Activists should be mindful that mobile phones present in homes, cars, and social settings might be gathering soft intelligence on social groups. If we were to make the recommendation that phones should be more frequently powered off, we might be laughed at for paranoia or for the impracticality of the suggestion. So-called liberal democracy gives the illusion that we do not live under a repressive police state, yet there are many cases where innocuous social circles and activists groups are hacked and surveilled, not to mention the more radical and involved groups.

Our suggestion is not that we should never have phones on our persons, but we do want to suggest that everyone become more aware of the effort the State and corporations expend to surveil and the utility of the information gleaned from casual conversation. There may come a time when repression heightens and we begin to feel its presence more sharply. To prepare for such times and to build habits that enable us to resist such repression, our suggestion is more moderate. Practice heightened security starting now. See if you can organize phoneless events. When you hang out or go hiking, even if you meet at a pub, see if you can get everyone to leave their phones at home. Accustom yourself to their absence. Feel the freedom of knowing you're not leaking location data to the State and that no one can hear your conversation except for those present.

CASE 3: SQUATTING AND SIMPLE PHONES

SCENARIO

A crew of activists want to squat an unoccupied building with the goals of drawing attention to speculative property investments, and if the squatting is successful, turn it in to free housing for locals who have recently been evicted. One team will be in the building doing the occupation, and other teams will be on the ground out front negotiating with the landlords and State agents and posting to social media.⁴⁴

ASSUMPTIONS

The occupation team thinks that the police could learn their identities by seeing what phones are communicating from within the building, and even if they are not arrested or prosecuted for this action, that knowledge could be used against them in the future.

COUNTERMEASURES

To reduce the chances of their identities being learned in the case where they are not arrested during the action, the occupation team has chosen to not bring their personal phones. They will only bring one “burner phone” to have comms with the negotiation team so that they can be involved with the decisions, to send posts to the social media team, and to have a sense of security instead of being isolated until the end of the action. They will be using a phone with a SIM that is not registered to any of their names to make themselves anonymous.

ANALYSIS

The crew is correct in not bringing personal phones into the building they are occupying as those could be used to identify them. Police could do this by looking at what phones are in the building, and seeing to whom they are registered or looking at where they tend to spend the most time (e.g., when their user is at home sleeping). The crew is incorrect in calling the phone a burner phone as its repeated use can be used to tie it back to the crew and individuals. This phone is more accurately described as a demo phone. Since some of the crew is remaining outside of the building without masks, the crew’s identity is known even if not all of the identities of the occupation team are known. If the phone is a personal “burner” belonging to one activist, and this phone has been turned on at the activist’s home, this could be used to prove that the activist was inside the building or was involved.

⁴⁴Is there value to live-posting such actions to social media? Dubious. But that’s another discussion entirely.

The crew have overlooked the security implications of using a simple phone to communicate with the negotiations team. The police may deploy an IMSI catcher so that they can read the SMS messages sent back and forth between the occupation team and the negotiation team. This may give the police a leg up in the negotiations or give them opportunities to exploit division within the crew to allow them to more easily force an eviction.

However, if the police are likely to expend this level of effort on tracking down the individuals based off of the phones present in the occupation, there is likely a strong enough push for “law and order” that the occupation itself would not even be a viable action.



Not the case in question. Just a cool photo.

RECOMMENDATIONS

The reasons the occupation team wanted to bring a single phone into the building were legitimate, but they should have used a demo phone⁴⁵ with a single use account they created on an E2EE chat app. This account should only communicate with one anonymous account belonging to the teams outside to prevent leaking the crew’s social network if the phone is confiscated or the app developer has data for those accounts that is later subpoenaed in court.

CASE 4: SIMPLE PHONE + SIGNAL DESKTOP

SCENARIO

Ruben is an activist involved with a crew he believes is under active surveillance due to their anti-government stances. To minimize how much intelligence agencies and local police can track him, he uses a brick phone with a SIM card when he is out and about. Because some discussions with his crew are more sensitive, they need an encrypted messenger and have chosen Signal. Signal requires registering with a phone number and will only generate the initial encryption keys on the iOS and Android apps. To get the Signal desktop app to work on his laptop, he has used the SIM card from his brick phone in his friend’s smart phone to set up an initial key pair

⁴⁵Or several demo phones, either with their own mobile connection or connected via a WiFi hotspot. The security properties of one versus several are nearly the same.

that he could link with his desktop app. Afterwards, Ruben signs out of his account on the Signal app on his friend's phone.

ASSUMPTIONS

Ruben's decision to not carry a smart phone is based on the belief that smart phones are more trackable than basic phones. Ruben also assumes that Signal is more secure than telephone calls or SMS, so he uses Signal for some of his communications.

COUNTERMEASURES

Ruben's decision to use a basic phone is intended to minimize location tracking from his smart phone. His decision to use Signal desktop is intended to prevent interception of his sensitive messages with comrades

ANALYSIS

Ruben's location is roughly as equally trackable when using a basic phone as with a smart phone. His communications are more insecure because he does not have the possibility that "emergency" messages can be sent to or received from members of his crew using his basic phone, and if he does, they will be intercepted and stored by the State. His countermeasures against surveillance have created a burden for both himself and his crew, and they have not made him more meaningfully secure against the threats he faces.

RECOMMENDATIONS

Ruben should use his own smart phone for communications in general. If there are times when he needs his location to be hidden or his conversations to not be eavesdropped on, he should leave his phone at home.

CASE 5: PHONELESS PLANNING

SCENARIO

The members of an affinity group have been actively involved in the liberatory movements for long enough that they are known to the State. They are currently planning Something Big. They have a ban on discussing it over electronic means; they only discuss it in person.

ASSUMPTIONS

They have assumed that the State would go to great lengths to prevent their action and even greater length to investigate it after it occurs. They assume it's possible that their electronics have been compromised by State malware. They assume that even absent any evidence, they will be on the list of primary suspects for the action, so their OpSec for the action needs to be airtight.

COUNTERMEASURES

Because of the possibility of malware, they are treating their electronics as less-than-trusted. Because of the possibility of targeted investigations, they do not discuss their action in their homes, their vehicles, or known social centers and spaces tied to liberatory movements. To help reduce metadata that links them together, they turn their phones off before they arrive at their meeting locations and turn them on again only after they've left.

ANALYSIS

The group is right to assume they may be under targeted surveillance, and they are right to treat their phones as snitches. Turning their phones off does decrease the possibility of malware using a microphone to spy on them, and it does create some deniability about their locations during the meetings. But this absence of information may be abnormal compared to their regular phone usage, and all of their phones disappearing roughly at the same time around a location could be a hint to the State that during these gaps something noteworthy is happening. This could create incentive for additional surveillance such as bugging the location — if they use the same one repeatedly — or sending a plainclothes spook to wear a wire and follow them in to the cafe or bar where they meet. Moreover, if one member of the group is caught but says nothing during interrogation, police could look at their phone records for anomalies. The police could query the data by asking the questions: At the times when this phone went off, what other phones went off near it? And what were the phones of our other suspects doing at that time? This could reveal the rest of the members of the affinity group, or provide supporting evidence that members of the affinity group were the individual's accomplices. It is possible the police do not think to ask these questions or that this is not part of standard operations, but it is better to leave no trail.

RECOMMENDATIONS

Because they are anticipating targeted surveillance and resources to investigate their activities, they should leave all electronics at home and pick random locations for their meetings that are either very loud or very isolated.

CASE 6: PHONES AT MASS ACTIONS

SCENARIO

Cass is an activist who primarily attends larger demonstrations, and while she is not radical herself, she has some friends who are, and she is generally aware of what they do. Fascists have planned a march, and Cass and some friends are going to join the crowds who hope to block their planned route. In order to connect with her friends

and get up-to-date information about the blockades or changing routes, Cass will bring her everyday phone (the only one she has).

ASSUMPTIONS

Cass is not worried about arrest because at similar actions in the past, when a large crowd of people who do not appear to be classically antifa block the streets, police only kettle them or drag them out of the way before rerouting the fascists. She does not think that if she was arrested they would look through her phone at all, legally or illegally. She is also not concerned about her phone's location data.

COUNTERMEASURES

Cass has taken no countermeasures against her location data being collected or phone being confiscated.

ANALYSIS

At mass actions, police may use IMSI catchers to see who has attended these protests so they can build profiles. This location data may be used to prosecute people for rioting even if the charges don't lead to conviction.

If Cass is arrested, which still may happen if the blockades are too small or she's one of the unlucky ones to get snatched while they form on the streets, she may have her phone searched. From this, police may learn of her social network or the activities of her more radical friends. This can endanger them more than her.

RECOMMENDATIONS

Even though Cass does not anticipate arrest, she should be more cautious with her phone. She could agree to meet with friends at a fixed place and time before the demo so that they can avoid bringing their phones at all, or if they really want to have real-time information, only one person in her group should bring a phone. Being careful with her phone can protect her radical friends who might engage in more militant means of resistance to the fascists.

However, the chances of any of these things happening is low, and the perceived benefit of bringing a phone is high. That makes this a case where it's "fine" for Cass to bring her phone... until suddenly it isn't.

In either case, make sure a good PIN or password is set and notifications are disabled.

CASE 7: GENERAL PLANNING AND COMMUNICATIONS

SCENARIO

A collective organizes legal protests and hands out flyers promoting green and ecological alternatives to the current status quo such as going vegan, better funding for bicycle infrastructure, and decreased reliance on personal automobiles. They use an e-mail list hosted on a server provided by some local techy activists.

ASSUMPTIONS

The collective assumes that police are generally interested in activists, but that the collective itself is not specifically being targeted. They know that local trolls like to harass the “woke hippie communist faggots.” They also know that there are other more militant green organizations in their region, and that members of their collective may be in all manner of other groups.

COUNTERMEASURES

The collective wants to avoid harassment, so they keep their e-mail list private and invite only. They want to avoid tracking by large e-mail providers, so they self-host their e-mail.

ANALYSIS

E-mail lists are largely popular because everyone has access to e-mail, but there are many different chat apps and not everyone uses the same ones, so collectives tend to continue using e-mail lists. Often people claim to have insufficient room on their phones for more apps. Some members of collectives have low technical skills and do not want to learn other apps, so sometimes e-mail is unavoidable.

Eco-activists worldwide, including in western so-called democracies, are specifically targeted for surveillance even when not engaging in direct action. Self-hosting the e-mail list may decrease corporate surveillance, but there is always some weak link with subpoenas for data. A large provider might comply without notifying the collective, and while the techies who run the server for the collective would likely quietly let them know even if they had a gag order, the police could circumvent this by going directly to the server’s hosting company and subpoenaing them. Further, the techies might not have the technical competence of large e-mail provider to keep the server secure or even notice if it gets hacked by trolls or the State.

RECOMMENDATIONS

If space on the phone is an issue, the activists should backup their photos and videos, then delete them to make space. This is generally a good practice to help save data in case the phone is lost or breaks.

The collective should ideally move to an encrypted chat app, but if they continue to use e-mail, it should only be for the most basic details such as the times and location of their activities. Planning, internal debates, and significant discussion should stay off e-mail as this information can give the State great insight into the collective which can be used for disruption. Each member should create a secondary e-mail account for some compartmentalization with their everyday identity.

CASE 8: UNDERGROUND RAVES

SCENARIO

A collective plans underground outdoor raves during a pandemic. They ask people to wear masks, and think this is sufficiently safe with regards to spreading the virus. Police have a blanket ban on mass gatherings (except for work and other things that keep the machine of capital greased).

ASSUMPTIONS

The State has made active efforts to break up mass gatherings (of course, only of the working class and marginalized), but they will likely not retroactively look for evidence of these gatherings. They have the ability to gather real-time phone location data which they may use to detect several hundred people in a remote location. Police have informants who listen for things like this, and some people just like to snitch on others if they hear about something they don't like.

COUNTERMEASURES

The rave is not posted to social media, and information is requested to be forwarded to additional contacts only via private channels. In the info, people are requested to put their phones in airplane mode when they get near the designated location.

ANALYSIS

Not publicizing the event is an obviously correct step to keep police from learning about it on their own. Asking people to only spread the info to trusted contacts via private channels is also a great way to reduce risk, but all it takes is one person to forward a trimmed down message with just the location and time for the warning to be lost. Even if the collective knows this, it is a risk they must accept.

RECOMMENDATIONS

There is little the collective can do to prevent people from arriving with their phones left on, and there is little they can do to ensure the message stays only on the trusted and security-minded parts of the social web. This is a hard problem in security culture because the lack of OpSec for a fraction of the individuals can still take down the whole group, especially since the individual benefit of keeping a phone on is high but the risk to the individual is low. The organizers who put it on and brought the equipment are the most likely to face consequences. If the crowd scatters during a raid, they will likely avoid consequences. The best the collective can do is, before and during the event, to try to emphasize the risks and use shame to convince people that their actions might be responsible for ruining the rave for everyone.

CASE 9: DEALING WITH A WEAK LINK

SCENARIO

An affinity group targets nazis who harass people in their community. They have an agreement of not bringing phones to their late night actions. Felix, one of their most active members, thinks this is overly paranoid and refuses to leave his at home.

ASSUMPTIONS

The group has assumed that the State might use phone location data to investigate their activities. They also assume that Felix bringing his phone endangers them all.

COUNTERMEASURES

To prevent Felix from endangering them, they have put a hold on their activities until they can reach an agreement with Felix.

ANALYSIS

Felix's actions do endanger the group, and the group is right that they should not let him participate in their actions. If the group fully ceases their actions, more harm could come to their community, and the risk of arrest from phones could be quite low depending on how police investigate things in the group's region.

RECOMMENDATIONS

The affinity group could create a subgroup of members who agree to not bring phones to actions and continue their work. In parallel, they could work with Felix to get him to understand how and why bringing his phone creates unnecessary risk. They could discuss with him that his actions cause them discomfort and that his actions do not affect him alone. The group may be able to remain comrades with Felix, but they may need to exclude him from secret actions if he refuses to leave his phone at home.

CLOSING REMARKS

Technology is neither good nor bad, is not inherently liberatory or oppressive (at least most isn't). New tech creates new opportunities while closing off others. With phones, this is no different. Having access to instant communications and vast knowledge in our pockets is tremendously powerful, but it comes with the cost — in this world, at present — of increased surveillance.

You may think the State isn't surveilling you, but if you're involved in liberatory social movements — even loosely — it surely is. Protecting yourself can protect your friends, family, or comrades who are more deeply involved. You may think that the State is hacking your phone to tap your housing co-op's weekly meetings, but it almost certainly isn't. Maximum security at all times is unattainable, and aiming for it is taxing.

After reading this you might be tempted to say “But they'll track me no matter what.” The belief that any level of safety against external threats is impossible is called security nihilism. People who feel like this often take one of two paths. They may believe that no countermeasures work, so they keep acting and take no precautions, thus creating a self-fulfilling prophecy ending with their arrest. Or, they may believe in the supremacy of the State and become paralyzed with fear. Repression works not just because of the stick that hits us or prison that cages us, but also because of the anticipation of those punishments and our subsequent self-imposed inaction.

Any steps you take can protect you, and many of them are so simple that you can start applying them right now. At the very least, you can avoid dragnet surveillance by using common encrypted messenger apps and leaving your phone at home during demos or direct actions. Every step you take beyond those will require your adversaries to make more concerted efforts if they want to surveil or disrupt you. Time and resources are limited, even for the large intelligence agencies. Humans make mistakes, and computers break. Your adversaries are fallible, and you can significantly decrease the amount of data they can capture and what sort of insights they can glean from it.

Moreover, the State isn't always using the maximum theoretically possible surveillance methods. Just because it's possible for State actors to hack your phone or track it, they surely aren't doing that to catch you walking through parks after their closing hours. Even in cases where the State wants to use maximum surveillance, they may do so ineptly. Your threat model should account for the realistically expected response from your adversaries given their knowledge of your actions.

This zine didn't list everything you could do with your phone and the apps on it to reduce different risks. Consider this a solid starting point, and go beyond. Learn about how the police, fascists, and other adversaries in your area operate, and come up with a threat model for yourself and your crews. Discuss it at length with your comrades. Start with a few bits of OpSec knowledge and turn it into a security culture. Foster shared understanding and practices that lead to increased security against the

threats you're likely to face. Take concrete steps, but make them pragmatic. Start slow with just a few new things at a time until they become normalized, then build from there. A plan is only good if you carry through with it, and trying to rush many large changes into a group tends to be overwhelming and frustrating. Most successful plans are applied incrementally.

Beware of urban legends. Activist spaces are rife with them, and security is no exception. Ask "How?" and "Why?" when people make claims about surveillance or countermeasures. Base your threat model and your security plan on verifiable facts — or at least very probable conjectures with supporting evidence.

Use this knowledge to protect yourselves as you reshape the world.

RESOURCES

The follow is a list of resources related to phone security. Some of these we don't quite agree with, and you'll see they contradict us, but we're including them regardless to help provoke thought and show you competing perspectives.⁴⁶ The resources are alphabetically sorted.

Kill the Cop in Your Pocket and *Encrypted Messaging for Anarchists* (both 2024) by AnarSec is also similar to this zine with general security advice for using phones as well as how to set up encrypted communication channels.

The No Trace Project is a collection of anti-surveillance and security focused texts aimed at anarchists and other radicals. It is a useful starting point for learning about security culture or doing research on specific security practices. See: notrace.how.

The P.E.T. Guide: New Communication Infrastructure for Anarchists (2022) discusses peer-to-peer alternatives to Signal and how we might use them as replacements or backups for Signal. Delta Chat, for example, has come much further since then including the integration of Webxdc apps.

Privacy Guides (continuously updated) is site with details about how to use your phone and computer in reasonably private and secure ways with a focus on breaking free of Big Tech. See: privacyguides.org

Signal Fails (2020) looks at some of the social downsides of using Signal for everything. It also offers some basic security advice.

Surveillance Self-Defense (continuously updated) by the EFF is a reasonably up-to-date guide on basic privacy and anti-surveillance countermeasures. See: ssd.eff.org.

Turn Off Your Phone: And Other Basic Digital Security Strategies (2023) is a similar but less technical guide than this one.

What Should We Do if Signal Messenger Gets Blocked?: A proposal and strategy guide to using Delta Chat as a backup (2025) is exactly what it sounds like. It explains in greater detail why one should set up Delta Chat as a fallback or replacement for Signal. See: signal-contingency-plan.info.

⁴⁶Intentionally omitted from this list is Activist Checklist (activistchecklist.org). They present themselves as by and for anarchists, but multiple people have said they are totally unresponsive to outside feedback (including from contributors to this zine). Their presumed threat model is a little closer to that of an average protester or organizer, and some of their advice is incomplete, insecure, or advocates for harmful practices or services without noting any caveats (such as recommending Brave and Proton). Follow their guides with skepticism if you choose to look there.

hakan-geijer@riseup.net /// opsec.riotmedicine.net

September 2026