Mobile Phone Security

For Activists and Agitators

Håkan Geijer

2022-05-03

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 State security apparatuses and private individuals. Those who are active in liberatory movements are aware—to varying degrees—of this surveillance, and collectively we have developed operational security (OpSec) practices and an internal security culture to counter disruptions to our efforts to organize.

There are many urban legends around phones use that stem from inaccurate understandings of the technology used by phones and 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 countermeasures. Action taken based off misinformation can lead to easy 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. It is not a binary that is either "on" or "off," nor is it even a spectrum of "better security" or "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 it is harm reduction. It may prevent your

imprisonment or save your life or the lives of those around you.

This zine was written at the start of 2022 by anarchists in Europe and North America, 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.

Your Phone and You

Your phone[1] 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. 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—to some degree—have also 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.

Compromise of a phone—either via confiscation or malware—by an adversary can be disastrous. All your photos, text messages, emails, and notes could be made available to this adversary. They could have access to all the currently logged-in accounts on your phone. 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 privileged parties such as the police who can request bulk or real-time access to metadata that is available to your carrier or ISP.[2]

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 because of what they enable, or should be 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.

[1] To save space, we are using "phone" to mean "mobile phone" or "cell phone."
[2] Internet service provider

Phone Tech

In order to understand how phones can be compromised and used to facilitate surveillance, we need to have an accurate understanding of how the different technologies used in phones work, such as the phone's hardware, the phone's firmware and operating system, 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 transceiver towers.[3] 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 sector[4] the signal arrived. When a phone's distance from multiple towers is simultaneously measured, the network provider can triangulate the phone's location very accurately.[5] LTE networks can position a phone's position to within a few tens of meters, and 5G networks are able 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 (IMEI[6]) along with their subscriber's ID (IMSI[7]). An IMSI is typically stored on a physical SIM[8] card or eSIM.[9] 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

[3] Not all cellular sites are towers, but using the layperson term suffices.

[4] The cone-shaped area covered by a single antenna.

[5] This is called "uplink multilateration." And as a note, we're using "triangulation" to mean "multilateration" because in this case it's worth trading technical accuracy for understandability.

[6] International Mobile Equipment Identity.

[7] International Mobile Subscriber Identity.

[8] Subscriber Identity Module.

[9] Embedded-SIM, a chip integrated directly into the device.

data. For example, in most (if not all) regions, emergency services can be called without a SIM. Removing a SIM card from your phone **does not** prevent tracking.

Types of Phones

Most people who say "phone" and mean "smart phone," namely one with an operating system and apps that can be installed by users. A basic phone is the least sophisticated kind of mobile phone, the kinds seen in the early days of widespread mobile phone adoption that can only make phone calls and send SMS messages. Somewhat rare these days are feature phones. They are somewhere between smart phones and simple phones. They may have vendor specific applications such as an email client or internet browser built in. To differentiate feature phones and basic phones from smart phones, the term "simple phones" is used to describe the two former types.[10]

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 uses signals received from GPS[11] or GLONASS[12] satellites to triangulate the phone's position. Most phones use A-GPS[13] 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 or multilateration, measurements from these sensors can be combined to derive a current location from known previous location.

What this means is that even though GPS signals are passively received by a device, use of location services can broadcast a phone's location, and that turning off location services may not be enough to prevent an app or malware on your phone from coarsely determining your location.

[10] Some people use the phrase "dumb phone" to mean either all simple phones or just basic phones, so we are intentionally avoiding this phrase for clarity.
[11] Global Positioning System, run by the US Department of Defense.
[12] Global Navigation Satellite System, a GPS alternative run by the Russian Roscosmos.
[13] Assisted GPS.

Simple Phones

Many activists believe that using simple phones rather than smart phones is "more secure." Because a phone without GPS or location service can still be geolocated, simple phones do not offer significant protection from location tracking. Feature phones typically lack widely available text or voice chat apps, and by definition basic phones have no such capabilities. This means that only unencrypted SMS and telephone calls are available, and these are susceptible to interception in more ways than if they had client-server or end-to-end encryption. Basic phones, the seemingly least technologically advanced, may only have 2G capabilities which means that calls and SMS are trivially interceptable with only about €25 worth of consumer-grade equipment. Further, many of these devices may have hidden internet capabilities that send telemetry data back to manufacturers without users being aware.

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

Malware

Malware is malicious software. It is a program that does something you don't want and tries to hide its activities. Malware created by the State often has the goal of simply surveilling and spreading to other phones or even electronics like WiFi routers.

Old internet security training said that malware is installed by visiting dodgy websites or opening attachments on emails from unknown recipients, and while this is still true, the attack surface of your phone is far larger. Most, if not all, of your apps poll for notifications or wait for notifications to arrive from Google Play Services and then make requests to the app's servers. Some malware is zero-click meaning that it requires no user interaction. As an example, the Pegasus spyware from the NSO Group used a zero-click exploit and targeted activists, journalists, and politicians. Malware can be installed on our 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 believe your phone has been compromised, you will need to find a malware specialist who can help you determine this, and you may need to get a new 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 flavors: iOS for Apple devices and Android for everything else. iOS is proprietary with private source code. Android is a base OS with public source code that manufacturers can modify for their devices. Manufacturers' Android OSes generally have private source code. In addition, there are many full versions Android maintained by the open source community, most notably LineageOS.[14] GrapheneOS and CalyxOS are open source Android OSes that have a significant focus on privacy and security.

When a phone is powered on, the hardware starts loading the OS using a process where each step verifies the integrity of the software needed for the next step. 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 disabled otherwise the hardware would refuse to load the custom OS because it is not cryptographically signed by a 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, and once malware is deployed, it can be detected and rendered unable to infect new devices by updates to the targeted app or OS.[15] Because of this, it is more economical to write malware that can target many users. iOS has a limited number of

[14] LineageOS is the successor the popular but discontinued CyanogenMod.

[15] Additionally, 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, and also that that particular type of missile would be much more likely to be intercepted in the future. Militaries would be hesitant to fire so many missiles and would need to be much more strategic about their targets.

versions for a limited number of devices, whereas the Android ecosystem is much more diverse. This means that targeting Android users is less economical and more difficult for adversaries.

Our recommendations are as follows:

- For most individuals who are trying to avoid mass surveillance and low-effort hackers, iOS or stock Android are sufficient as they are easiest to use.
- 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 communications.
- For individuals who have attracted or expect to attract the attention of intelligence agencies, phones should be avoided for everything related to activism.

Device Encryption

iOS and Android offer the ability to encrypt your personal data. This goes under various names like Data Protection or Device Encryption. Phones generally **do not** have device encryption enabled by default. This feature **must** be enabled by the user either when the phone is set up or later in the settings. Likewise, the protection against excessive login attempts must also be enabled.

Device encryption implementations generally use a hardware security module (HSM) or a security coprocessor,[16] special chips in the phone that handle encryption, decryption, and the cryptographic keys used for these operations. These chips are important because they protect the keys from unauthorized access and tampering. These chips may impede adversaries from accessing your data, but it is no guarantee. The tool GrayKey—among others—is capable of exploiting bugs in HSMs, and in some case it 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. Device encryption does a good job preventing your data from being accessed if a chud gets access to your phone of if a cop snatches it during a stop-and-frisk. It is not likely to withstand concerted efforts from State intelligence agencies like MI5 or the FBI from accessing your data.

[16] On Apple devices, this chip is called the Secure Enclave.

A high profile example of this when the FBI cracked the password of 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.

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

A virtual private network (VPN), in the context most activists' use the term, refers to an application that routes a device's internet traffic to a service whose purpose is to obfuscate the user's web traffic and IP address from network observers or the servers that are being connected to. When used, VPNs will protect your traffic from snooping on public WiFi networks, and they will hide your IP address from servers you connect to. They can add some misdirection to investigations and make passive surveillance more difficult, but VPN apps can leak traffic, or you might forget to enable them. Traffic to and from your VPN provider can be correlated by State intelligence agencies who are able to view all internet traffic, and your VPN can be legally compelled to collect or turn over logs to law enforcement. VPNs are cheap, they can improve the security in a few ways, but they should not be relied on to provide anonymity against the State.

IMSI Catchers

An IMSI catcher[17] is device that spoofs being a legitimate cell tower and induces phones to connect to it thus allowing eavesdropping or the sending of SMS messages or phone calls. Sometimes this spoofing is detectable, but detection of them should not be relied on. In some regions they may be deployed without a warrant, in particular during demos. In part, IMSI catchers work by downgrading the protocol to one with no encryption or one with breakable 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 not robust against interception by IMSI catchers.

[17] Often IMSI catchers are referred to by the popular brand name StingRay.

Faraday Bags

Phones send and receive information using electromagnetic radiation. This radiation can be blocked by special materials. Urban legends and some supporting evidence say that signals can be blocked by putting a phone in one or more crisp bags[18] 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 phone signals.

If you need to transport phones and ensure that they are not leaking signals, turning them off may not be enough. Few smart phones can have their batteries removed. Something leaning on them in your bag might press the power button. Malware can hijack the shutdown routine and prevent the phone from actually powering off when you try to shut it down. Placing a powered off phone in a Faraday bag can prevent them from sending signals and will significantly reduce the possibility that the location can be determined.

Security Basics

There are some phone practices that tend to be advisable for most activists. A few are detailed here.

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. It may be annoying, but many updates contain security patches for critical vulnerabilities. If nothing else, this can prevent your bank, money transfer, or payment accounts from being drained.

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 webpages. However, these require some level of trust in the corporation offering the product. Free alternatives like KeePassX exist but do not have the ease of use that paid products

[18] Also known as "chip bags," for the yanks.

do. When using a password manager, all your accounts should have strong, unique, random passwords. These are typically automatically generated by the manager. The master password to unlock the manager should be a long, random phrase.

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!` 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. Five words is the absolute minimum, six is better, but anything over eight is overkill. Doing this provides unguessable randomness that you cannot create on your own, and moreover this randomness is easily memorizeable. An English-language, user-friendly wordlist is provided by the EFF. An example phrase is `MutableCalmBlubberFitJustify` (please **do not** actually use *this* one; make your own).

Table 1: Sample EFF Diceware Entries

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

Locking Your Phone

Depending on your threat model, you may want to make it difficult or near impossible to unlock you phone. This is of particular importance because the unlock method is also the decryption method, so a strong unlock method helps defend against unwanted access to your data if you phone is captured. In general, you should prefer passwords to either PINs or 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. In some regions there are legal protections for passwords but not for fingerprints or other biometrics.

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 notifications from 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 your unlock password has not yet been entered). 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. You can do this before interactions with law enforcement, going to bed, or leaving your phone unattended.

Wireless Features

You may want to disable WiFi and Bluetooth when you are not using them. Both of these can be used for "fingerprinting" and identifying your phone. Additionally, they increase the attack surface available to hackers who are attempting to break in to your phone. While the risks from leaving them continuously enabled are minimal, these practices can add marginal improvements to your security, and 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). Apple has previously halted plans to encrypted backups in their iCloud following pressure from the FBI, and their backups are unencrypted. Google offers end-to-end encrypted backs that, following external reviews, offer strong assurances of privacy from Google itself or law enforcement. Additionally, some apps may have their own backup services. For example, WhatsApp can backup your conversations to its servers.

Our recommendations are to avoid backups to Apple, but backups to Google are safe enough because you should not have incriminating evidence

on your phone anyway. Because data that is sent to third parties may still be lost or destroyed even if it can't be recovered by police, you should consider backing up your data to an encrypted hard drive you keep at home or somewhere safe.

Messenger Apps

Messenger apps provide more secure 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,. your phone) and the server is encrypted and protected from interception or tampering. The message is decrypted and 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 with the server only acting as a blind relay because the messages are only decryptable by the other client.

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 metadata about the size of the message, the time it was sent, its sender, and its recipient.

Some messenger apps offer opt-in E2EE such as Telegram with their secret chats, but this feature is not available for groups. Other apps such as Signal or Wire have mandatory E2EE, as do iMessage (Apple) and WhatsApp.[19] Some apps like Element have E2EE enabled by default, but it can be disabled for compatibility with older clients.

The security of E2EE depends on verification of the exchanged keys which is often done by scanning QR codes containing a fingerprint that is (statistically) unique to the generated key. Some apps require you to only verify one fingerprint for all devices, but others require you to verify one fingerprint for every device. Some apps send notifications in the conversation

[19]There are more interesting peer-to-peer chat apps like Briar and Cwtch that are metadata resistant and possess other interesting security properties, but they do not have wide adoption. They are also not available for iOS which prevents most crews from using them for secure comms.

notifying you when your contact's fingerprint changes, possibly suggesting something nefarious. Some apps unfortunately do not do this. You **must verify** all fingerprints for all devices, and if a fingerprint changes, **you must re-verify it** otherwise all of your security 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.

2B **C6** DE **D5** 12
CF **B0** 69 **10** 56
8C **FB** 1D **8F** 60
B5 **03** 1D **60** B5

Figure 1: QR Code and Fingerprint

Usage

The mantra "just use Signal" is often repeated by activists, but it falsely assumes 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 doing so may flag a user as suspicious. In North America and Europe, these drawbacks generally do not exist. However, there are common complaints against Signal such as that it requires a phone number to register, and that contact lists are shared with the server in merely semi-secure ways to allow for contact discovery and initial key exchange.

For most apps, when messages are received, they are decrypted and stored in plaintext on the device. Some apps like Signal allow you to set a password to prevent access to the message while someone else is using your phone, but this does not re-encrypt them in any way. If device encryption is enabled on your device, you regain some privacy over these messages as discussed in the device encryption section.

Because messages are stored in plaintext, and because they might be recoverable even with device encryption, you likely 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.

What this means is that you should strongly prefer text and voice chat apps that have mandatory E2EE unless there is a compelling security reason not to, you should verify keys before messaging, and you should likely enable disappearing messages.

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 message. 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 comms from being read.[20]

Figure 2: Input Method Editor and Pinyin Candidates

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 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.

[20] Further, 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.

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

While we have strong criticism for Signal here, this criticism is 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.

Email

There are ways to make email communication more secure, but email as a protocol and communications medium is generally not secure for private communications. Boutique and activist-friendly email providers (i.e., non-Gmail/non-Microsoft/etc.) do not offer significant security benefits against interception by law enforcement or hackers. When sending emails, some people use PGP or S/MIME, but these are difficult to use and have an overall poor user experience. Two people using these encryption methods can have fairly good protection against having their email read, but one misclick can send the entire history of a conversation in plaintext thus making it viewable by law enforcement. ProtonMail has made bold claims about encryption for their emails and clients, and many activists have taken these half-truths to mean that using a ProtonMail account means *all* of their email are encrypted, but this is not the case. Email should generally be avoided for planning and especially for secure communication.

That said, email remains popular because every device can send and receive email, and some people "don't do chat apps." For coordinating a local tenant's union or setting up shifts at the local infoshop, email may be fine. If you choose to use email, 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 that can be exploited by the State.

Finally, there are legitimate use cases where email 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. In cases like this, phones should still be avoided because of their ease of trackability.

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 used 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 programming errors or user errors from exposing your private information. 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. You may make a mistake and reply to a social media post from the wrong account. When you click on an email address intending to use one of your aliases, your phone's OS might start composing an email with a default email 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 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.

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. These are spyware apps, 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 of loss can be devastating. A number of approaches are used by activists—and others—to help reduce their risk even if they cannot fully articulate their risk or why their 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 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 user to have maps and E2EE communications.

Activists erroneously use the phrase "burner phone" to describe demo phones, disposable phones, or any simple phone.[21] A burner phone takes its name from the fact that it is single use and after that it is destroyed. 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.

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

1. The phone must be purchased[22] using cash.
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 user 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 and SIM card must be powered off after the action then immediately destroyed.

[21] People 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.

[22] Theft 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, 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 making calls or using data.

A complicating factor is that some phones or SIM cards require activation either by calling a number of 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.

When we say that a burner can be used for one action, we mean "one time-boxed sequence of activities." This may mean one direct action that takes place over only two hours. It also may mean the planning and coordination in the month before an action as well as the action itself.

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 creates the additional possibility that the stored security footage of the purchase could still be accessible.

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 in a short time frame. Gradual activation is less detectable when the State analyses 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.

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 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, 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 do that. But at the same time, don't let others' poor security endanger you. Find a balance.

This is by no means an exhaustive list, but are some ways to develop personal OpSec 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 E2EE encrypted apps for communication, enable disappearing messages, and avoid email.
- 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, emails, 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.
- Start all meetings by establishing whether or not electronics are permitted. If not, power them off, collect them, and move them out of range of your conversation.

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, it's use could make you a target. VPNs may be criminalized. Use of Tor may get your 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 is that people want to have info, gather info, and trade contact info. A pen and a note pad and let you have your collective's meeting minutes accessible in an analog 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 to avoid creating a literal paper trail of your activities.

Phoneless Contingencies

While your plan may work today, it 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 are fallbacks, and your planning needs to incorporate the possibility that this will the only way to move 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 more accurate 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 collected and placed in a sealed plastic box 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 box, then having a loud conversation to see how much is understandable. If the voices are remotely recognizable, snippets could 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 could record the conversations.

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 at fixed location from 19:00 to 21:00 on Wednesdays for many consecutive weeks.

Recommendations

If phones are collected to prevent surveillance, they should also be powered off. There should be loud, ambient noise where phones are placed to minimize the chances that they can pick up the audio of the conversations.

If the group believes they may be prosecuted for conspiracy to commit a crime, the may want to leave phones at home or power them off before traveling to the meeting. This can be further minimized by not bringing the same phones to the action itself.

If high security is desired, 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 and 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 was like for organizing to increasingly take place where everyone effectively had 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 expends 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 activist 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 State and posting to social media.

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 brining personal phones into the building the are occupying as they 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.

The crew have overlooked the security implications of using the basic 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.

Recommendations

The reasons the occupation team wanted to bring a single phone into the building were legitimate, but they should have used a demo phone with a single use account 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 basic 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 basic phone in his friend's smart phone to set up an initial key pair 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, and 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

Isa 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 Isa 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, Isa will bring her everyday phone (the only one she has).

Assumptions

Isa 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

Isa 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 Isa 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 radial friends. This can endanger them more than her.

Recommendations

Even though Isa 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 Isa to bring her phone... until suddenly it isn't.

Case 7: General Planning and Communications

Scenario

A collective organizes legal protests and hands our 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 email 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 "hippie communists." 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 email list private and invite only. They want to avoid tracking by large email providers, so they self-host their email.

Analysis

Email lists are largely popular because everyone has access to email, but there are many different chat apps and not everyone uses the same ones, so collectives tend to continue using email 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 email 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 email 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 email 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 email, 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 email as this information can give the State great insight into the collective which can be used for disruption.

Case 8: Underground Raves

Scenario

A collective plans underground outdoor raves during the corona virus 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 secure means. 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 in secure ways is also a great way to reduce risk, but all

it takes it 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 to do 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 try to use shame before and during the event 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 brining 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 not good or bad—at least most isn't. It's not inherently liberatory or oppressive. 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 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 move deeply involved in the movement. 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 this often take one of two paths. They can 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 can believe in the supremacy of the State and become paralyzed with inaction. Repression works not just because of the stick that hits us or prison that cages us, but also because of the fear 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 easiest, you can avoid dragnet surveillance by using basic encrypted messenger apps and leaving your phone at home during demos or direct actions. Every step you take

beyond those will require your adversaries 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 adversary is 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 the State 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 realistic expected response from your adversaries given their knowledge of your actions.

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.