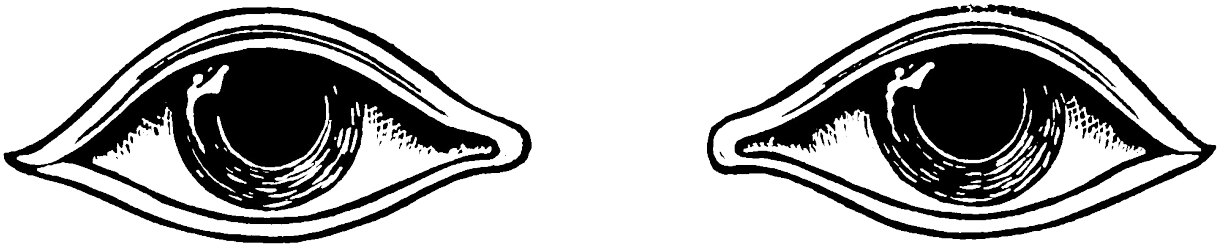


OCTOBER REBELLION PHONE LOCKDOWN

Have a laptop? be sure to read the Laptop Lockdown

Taking your phone to an action

So, you've decided to take your phone to an action. Before you do, we'll need to ensure it's safe to do so...

Very few phones *only* have data belonging to their owner on them: most have many contacts, photos and videos of other people - the people in our lives. While you may feel little concern for losing the data on your phone, others may not feel the same way, and may be harmed unless your phone is sufficiently secured from data theft. This is especially pertitent to those engaging in civil disobedience. More so, if you're an XR coordinator you probably have a large contact list that can be used by an adversary to deeply harm your branch. Logins to important accounts on the phone can also be hijacked/compromised.

Activity: let go of your phone

Find a quiet place and put your phone in front of you on the table, with the screen facing down. Take your hands away from it and look at it. Imagine seeing that phone taken from you by a police officer, who then puts it in a bag. Imagine you will never see that phone again, with experts at the police station later going through that phone, copying off pictures and videos (if it's a modern phone), all your contacts, and texts, opening up the browser to log into your social media and XR platform accounts. Perhaps they find the MicroSD card and take that out too.

Meditate not just on *what* is on that phone, but *who* is on it, and what other *accounts* (and information) that phone can be used connect to. Think also about how all of this might implicate other rebels not just at that action, but in the future, even when they may no longer be part of our movement.

In summary, **we don't only lock down our phones for ourselves, but out of caring for each other and our branch**. Respecting privacy and anonymity is also essential to our regenerative culture in a time where such basic rights are so widely exploited by corporations and governments, used to control, disempower, and condemn.

GET EMPATHIC ABOUT DATA

- Photos, videos and audio recordings of rebels, especially at A&L meetings
- XR account login details (Mattermost, Base, email, Pads, etc)
- Contact lists

Ask yourself

“Do I *need* to take my phone to this action?”

Older style phones (’dumbphones’)

Dumphones are very hard to secure as they offer no opportunity to internally encrypt their contents. With that said, the limited storage and application capability of dumbphones usually ensures there’s much less to lose than on a modern device.

IMPORTANT: Extracting contacts and other information from dumbphones is trivial. Be sure to erase all contacts from the phone and its SIM card and only have contacts you need for the action on the device or SIM card.

Smartphones

Securing iPhones with Encryption

Most modern Apple (iOS) phones already come with the contents of the phone encrypted. However that doesn’t stop someone that has your device accessing the data on it. For this reason the encryption needs to be password protected, such that without it the data is inaccessible.

IMPORTANT: If you choose a passcode that’s all-numeric, you will get a numeric keypad when you need to unlock your phone, which may be easier than typing a set of letters and symbols on a tiny virtual keyboard. However, we suggest choosing a passcode that’s alphanumeric, and longer than 8 characters because it’s simply harder to crack, even if Apple’s hardware is designed to slow down password-cracking tools.

iOS4 to iOS7

1. Open the General settings and choose Passcode (or iTouch & Passcode).
2. Follow the prompts to create a passcode.

iOS8 and higher

If your device is running iOS 8, disable Simple Passcode to create a code that is longer than 4 digits. With the release of iOS 9, Apple defaulted to a 6-digit passcode.

To customize your passcode, select “Passcode Options” and “Custom Alphanumeric Code.” If you want to customize an existing passcode, select “Change Passcode” and then “Passcode Options.” You should also set the “Require passcode” option to “Immediately,” so that your device isn’t unlocked when you are not using it.

Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says "Data protection is enabled." This means that the device's encryption is now tied to your passcode, and that most data on your phone will need that code to unlock it.

Apple backups: a warning

Apple device owners commonly backup either to the Apple iCloud or iTunes.

IMPORTANT: If you backup to the iCloud, you should consider all that data accessible by Law Enforcement. While Apple will tell you the data there is encrypted, they have the encryption keys, and are obliged to comply with the jurisdictional process in the event of a criminal investigation. For this reason this option should be avoided entirely.

If you backup your Apple device to your computer using iTunes, it is important to know that the iTunes backup system does not encrypt the data by default. For this reason you should choose the *Encrypt backup* option such that all the data is encrypted when it is stored on your computer. Be sure to remember the passphrase you choose and to use whole disk encryption for your laptop.

Securing Android phones with Encryption

Device encryption works in the much the same way across all Android devices, but the methods for enabling it have changed a little over the years. Most devices come with encryption enabled

by default these days, particularly those running newer versions of Android. For example, every Pixel smartphone, the Nexus 6P, the Nexus 5X, and even the Nexus 6 and Nexus 9 have encryption enabled by default. If not, Android makes this a very simple process.

Android 5.0 and higher

For Android handsets and tablets running Android 5.0 Lollipop or newer, you can navigate straight to the “Security” menu under settings. Getting here might be slightly different depending on your OEM, but with stock Android this can be found under Settings > Personal > Security.

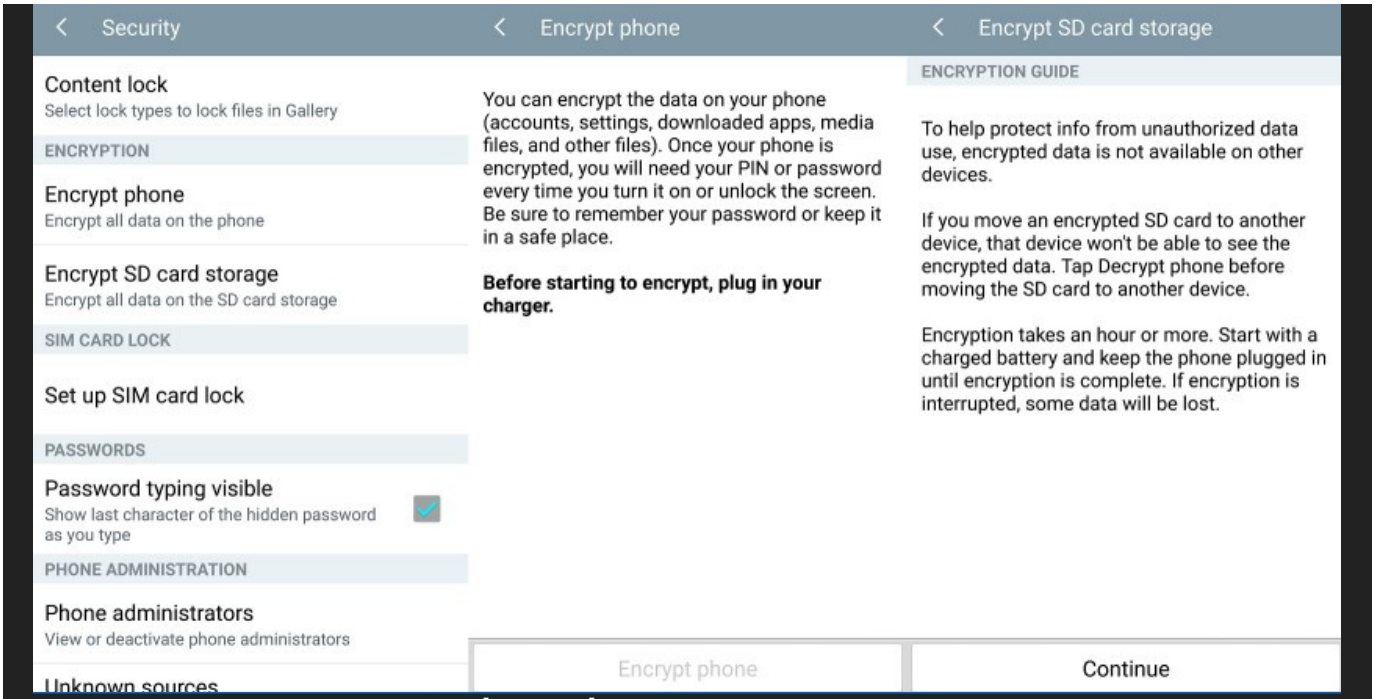


image.jpg840×443 94.6 KB

Here you should see an option to *Encrypt phone*. You’ll be asked to plug your phone in to charge while the process takes place, just to make sure that your phone doesn’t shut off and cause errors. If you haven’t done so already, you will be prompted to set lock screen PIN or password, which you will need to enter when you turn your phone on or unlock it in order to access your newly encrypted files.

Android 4.4 and lower

If you’re running a handset with Android 4.4 KitKat or lower, you will have to setup a PIN or password before starting up the encryption process. Fortunately this is simple enough. Go to Settings > Security > Screen Lock. Here you can either pick a pattern, numbered PIN, or mixed password for your lock screen. This will be the same password used after encryption, so make a note of it.

Once that’s done, you can go back to the Security menu and hit “Encrypt phone” or “Encrypt tablet.” You’ll need to have your phone plugged in and read through the warning messages, and you will almost certainly have to confirm your PIN or password one last time before the encryption process starts.

image.jpg1024×682 170 KB

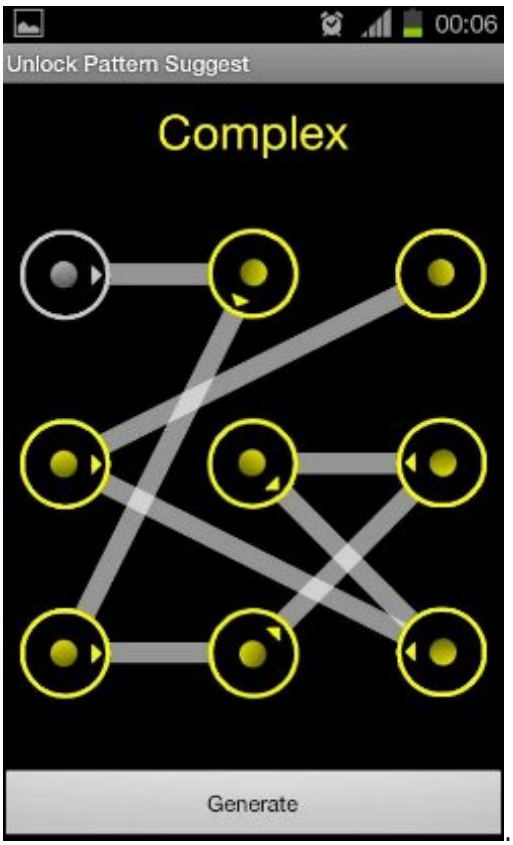
Encrypting your phone can take an hour or more, depending on how powerful your handset is and the amount of data that you have saved on the device. Once the process is finally finished you can enter your PIN and start using your newly encrypted device.

Back in the *Security menu*, you will also likely spot an option to encrypt files on your microSD card as well. This is a recommended step you want to keep all of your data secure. Please note that if you choose this option that microSD card will not be usable in any other device (like your laptop, or a camera).

Pattern Unlocking an Android Phone

A sufficiently strong password can be hard to remember and so people tend to use less secure, shorter passwords. With All android devices, however, there is an option to use a Pattern Lock for unlocking the phone. This is an excellent option as complex gestures are often more easily remembered than passphrases. Be sure the pattern has at least 6 lines, and consider using a more complex 4x4 (or more) dense grid.

A 3x3 grid however can be robust, assuming the pattern is sufficiently complex. Below is an example.



Android backups: a warning

Android devices are synced to remote backups using a variety of ways. All should be disabled, in favour of backing up to a local device (like a laptop), which itself should have full disk encryption. A section on laptop security will be available soon. Before going into an action features like Samsung's "SideSync" should be disabled.

IMPORTANT: Are you an app developer? Disable USB Debugging. Developers and geeks often use special features to manipulate their phone on a low level. Having *USB Debugging* enabled, for instance, introduces the very real risk of an attacker with physical access to the device being able to use Android's adb tools to gain access to the device. Be sure that *USB Debugging* is disabled on a smartphone before taking it to an action!

MicroSD cards

MicroSD cards can be easily taken from a phone, their contents analysed and copied. Be sure to go through all the contents of the card before taking it to an action. Assume anything on the card vulnerable.

IMPORTANT: Even if your phone is encrypted, your MicroSD probably isn't. On some phones it is possible to encrypt a MicroSD card. Be sure to check there is no dangerous data on your MicroSD card before taking it to an action, unless otherwise encrypted.

Communicating safely before & during actions

Two kinds of networks

Today there are two primary networks used for voice and text communication with other people using a phone: SMS and voice calls using a traditional mobile network (GSM, CDMA), or communication over the Internet, using apps and a mobile data plan (3g/4g), or a local WiFi connection.

When we are at an action, we very rarely have the luxury of a WiFi based communication, and so typically we'll be using a SIM card in our device to connect to a mobile network (whether to call or make SMSs) or using a data plan with an app (like *Signal*, *Wire*, *Telegram* or *WhatsApp*).

SIM cards are a little like license plates on cars: they are tied to an identity, often a bank account too, via your mobile provider's subscription. This can be a very fast way of identifying someone using a simple lookup even without Police needing to access the server provider's records GSM/CDMA traffic records.

For this reason, please consider using a *burner SIM* card in your phone. A burner SIM card is the name given to a disposable SIM that can be bought with cash and without handing over ID. This makes it much harder for surveillance operators and service providers to associate calls and texts from your device with you. SIMs can be bought with cash and no ID in many countries, but not all. LycaMobile is one example of an operator in Germany that will sell such SIMs in stores. Help your fellow contacts use burner SIMs and protect your SIM with a passcode, if you can.

Better still, use a Burner SIM with a Burner Phone (a 2nd hand phone bought with cash), as that way the phone's identity, the *IMEI*, cannot be linked to you either. All coordinators should consider the burner phone/SIM combination. For more information, see this post on the Global Base.

IMPORTANT: Avoid ever making XR-related calls, or send SMS (text) messages, using a mobile network unless absolutely necessary, and if so never give incriminating and identifying details over the phone.

Calling safely using End to End (e2e) encryption

End-to-end encryption refers to a kind of data privacy whereby the data is unreadable to any other than the people communicating at either end; no one along the way can have access to that data. There are several different apps that will provide you with e2e when making calls and sending text messages. *All of them require the intended recipient of your text message or call has the app installed and that you have already added them to the address book of that app.*

IMPORTANT: WhatsApp and Telegram are to be considered unsafe. Both have serious security issues. We recommend only using Signal or Wire for encrypted calls and text at, or when

planning, actions.

Signal (OpenWhisperSystems)

Signal has an excellent reputation in the information security scene and enjoys increasing use. Its rapid adoption has been partially due to the contact-discovery system which uses people's phone numbers. That way you can simply input a friend's phone number and invite them to join Signal. You can also find a friend already using Signal with their phone number.

Signal has group chat, voice and video calls, and is widely used among branches in XR to secure their mission-critical communications.

The system of using phone numbers, however, is not without its risks for activists. If your phone is compromised and/or insufficiently secured, it is easy for an adversary to find out who you have been communicating to using Signal.

IMPORTANT: If you choose to use Signal, connect it to a *burner SIM* (a SIM card you've bought with cash, and without handing over your ID) phone number, if possible. Secondly, use the Signal feature of protecting access to the app with a *pattern lock* such that it makes it that much harder for someone to get to your contacts list.

You can download Signal for iOS and Android, here. Note there's also a desktop version of the software, which is particularly convenient if working across laptop and phone.

IMPORTANT: Only install Signal on your laptop if your laptop is sufficiently secured as all your Signal contact list and messages will be available on your laptop.

Wire

Unlike Signal, Wire does not depend on a SIM card to activate, and so while no more private than Signal, it certainly has more potential for anonymity. Wire offers chat, voice and video calls, and file sharing. A particularly unique feature is support for multiple accounts.

Something not going in Wire's favour is that significantly less people use it than Signal. This is partially due to Signal having a stable version of the app available much earlier. Another is that it is not possible to add a passphrase or pattern-lock to Wire to protect its contents from an attacker that has access to your running phone.

Wire will run on iOS 10.0 or Android 5.0 or newer. If you have an older device, and cannot upgrade, consider Signal. Note there's also a desktop version of the software, which is particularly convenient if working across laptop and phone.

IMPORTANT: Only install it on your laptop if your laptop is sufficiently secured as all your Wire

contact list and messages will be available on your laptop.

You can get Wire here.

Briar

Briar was last to the Smartphone counter-surveillance space but with perhaps with the most unique offering. Unlike all other e2e encrypted messaging solutions for phones Briar does not specifically depend on traditional network infrastructure to function. Built for activists, it assumes operational conditions where statecraft have disabled and/or jammed cellular or WiFi networks in the vicinity of an action or protest, as has been broadly documented in Turkey, China, USA and Ukraine, to cite a few.

To do this, it leverages the BlueTooth functionality on almost every smartphone, to push messages from device to device, in a *mesh-network* fashion: a significant advantage in a coordinated effort to disable the communication infrastructure of a sustained action, assuming police do not have physical access to all participants and can simply seize their devices.

When access to the Internet is available, Briar will use the anonymising Tor Network, adding an extra layer of cover, in that it cannot be proven that any device was the source of a transaction with another.

You can install Briar here.

Securing the login to your phone

One of the best ways to ‘think security’ is to imagine our device in the hands of an adversary, one that might seek to incriminate you, your branch, or members of your branch.

Rules for all smartphones

1. DO NOT USE A PASSPHRASE USED ANYWHERE ELSE TO ACCESS YOUR PHONE

If you use the same log in with your bank that you use to unlock your phone, and a federal investigator is granted access on a warrant to all data related to your bank account (very common), your phone can be unlocked by police. For this reason it is always a good idea to use a different passphrase, assuming you wish to use a passphrase and not a pattern lock (Android). Make the passphrase longer than 8 characters, and alpha-numeric, where possible.

2. DO NOT USE BIOMETRIC LOGIN (LIKE FINGERPRINT OR YOUR FACE)

If you are arrested it is assumed that police will have access to your body, under force, to log into your device if you have chosen to set your device to use biometric login. It has already happened that rebels arrested in France were held by police officers and their phones logged into simply by an officer taking their phone as another held the rebel, and their face was used to access the device. The same has been done with fingerprint-based login. These login methods should be avoided by activists.

3. NEVER STORE PASSWORDS UNENCRYPTED, OR IN THE CLOUD. ONLY STORE THEM ENCRYPTED AND/OR IN YOUR MEMORY

It is advantageous to have a backup of your password to your phone, but very disadvantageous if your adversaries have access to it. Do not use services like *LastPass* or *iPassword*, as they store your password remotely, with the former being catastrophically hacked, compromising countless trusting members. Even though iPassword state they do not have the ability to decrypt your password and so read it, you have to trust them. This is putting your wellbeing in the hands of those you’ve never met, a business in a country under its own jurisdictional obligations to cooperate with law enforcement and federal investigators.

By sure to use an offline password manager, like KeePass or KeePassXC which stores passwords encrypted and on your device (like a laptop), under your control.

There is no problem storing the password to your phone on your laptop, but only if your laptop uses a secure means of storing that password.

Pre-arrest checklist for branches

1. DO NOT LET PLATFORM ADMINS AND SYSADMINS GO TO ACTIONS

While this may be very disappointing for admins and sysadmins, they are to be considered extremely high-value targets and if known to police they may be subject to extreme coercion and/or incarceration. **Sysadmins especially should be forbidden to go to actions**. Further, an admin in jail is not available for their branch, something can be ruinous for branch operations. Sysadmins and admins should be online the entire time to assist during platform lockdowns (see below).

2. NOMINATE LOCKDOWN CONTACTS

Each branch should nominate one or more Lockdown Contacts whose anonymised contact details should be available on each phone taken to an action. **This rebel's job is to ensure that arrestees are made immediately known to platform admins and sysadmins such they all their login sessions are revoked and their passwords changed.** The lockdown contact should be in a safe place throughout the action with good bandwidth/connection. They need to be reachable the entire time.

It is up to branches to define their own protocol for account lockdown.

3. CONSIDER DESIGNATED PHONE CARRIERS

Discuss with your A&L team the possibility of designating smartphone carriers to document actions, coordinate, stream and publish on social media, etc, while discouraging other rebels taking part in the action from bringing their phones. This can be a good way to minimise possibility of compromising data leaking into unhelpful hands.

4. STUDY THE LAW

All branches should assign a legal team to work *specifically* on rebel rights at the point of arrest. **Rebels can only be safely arrested when they are arrested knowing their rights**. A rebel that doesn't know it is illegal to be physically forced or threatened to hand over the login details to their phone probably will. Part of caring for each other is ensuring that we are all on the same page, and can stand strong in full confidence we know our rights, and are not being lied to to compromise the safety of our peers.

IMPORTANT: it is very important to determine, within your operating jurisdinction, if it is against the law to withhold a passphrase from law enforcement at the point of arrest. If this is the case, it is essential all rebels are aware of this, and that all devices with any sensitive information are not taken to an action, whether encrypted or not. Withholding information from law enforcement - 'obstructing legal process' - is generally an offense much more serious than blocking a road, and in some jurisdictions can result in being imprisoned for many years, or worse.

Pre-arrest checklist for rebels

1. DO NOT ATTEMPT TO CALL ANYONE, EVEN YOUR LOCKDOWN CONTACT, UNLESS YOU HAVE PLENTY OF TIME

What constitutes “plenty of time” is of course awfully subjective, but as long as you have time, with ease, don’t hesitate to make that call. If not, call it quits and go to 2.

2. PRESS THE POWER BUTTON ON YOUR PHONE AND ENSURE IT IS POWERED OFF BEFORE HANDING IT OVER

If you have reason to believe there is any risk of your smartphone coming into the hands of law enforcement or investigators, be sure to hold down the power button and power your phone off. **Only when an encrypted phone is off is it truly (practically) invulnerable to data extraction.** Do this also when crossing a border.

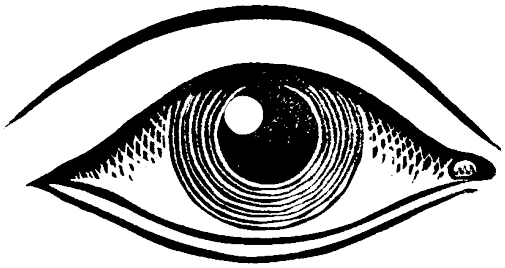
3. RECITE YOUR RIGHTS

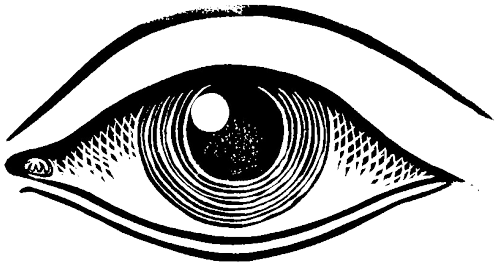
While not easy when you’re being dragged away, try to go over your rights in your mind. Recite them to yourself, before saying a word to law enforcement.

IMPORTANT: If Police do return your phone to you and your phone is not encrypted, it should be considered compromised and so totally wiped. Malware implants in activist phones are increasingly common, allowing investigators to spy on you, activating your microphone or copying data from your phone.

Leaving your phone at home?

So, you’ve chosen to leave your phone at home. Great move! Not only do you not risk losing it to Police, but all your account logins and contacts are not exposed to those that might use it against you and/or other rebels. Please consider encrypting your device nonetheless. Post-action arrests are a reality, and encrypting a phone makes the phone’s contents impervious to someone that has it, when the phone has been powered off first.





Afterword

This guide is still in draft. It is intended solely to protect rebels on the front-line at (and in the lead-up to) actions.

Route encryption with a VPN, anti-tracking and XSS mitigation, Stingray and rogue cell-tower detection, anonymity apps like Orfox, custom ROMs like LineageOS with MicroG for a de-Google'd setup, EXIF cleaning, etc are considered beyond the scope of this document, intended for non-geeks, and will be covered further in the Global Base in the Operational Security category.

If you have any suggestions as to additions or ammendments, please leave them in this thread on the Global Base. If you are not a member of this discussion forum, please write to support@organise.earth and ask the XR Global Support Team for an invite.