# Setting Up a Phone for Offline Documentation

*This post is part of a series on Documenting During Internet Shutdowns.*

Last reviewed: 31 January 2020

Despite an internet shutdown, documenters can still capture important video evidence that can be shared offline or when they are able to get back online.

Here are some tips that we've learned from activists and other practitioners to set up a phone for offline documentation. Note that some steps **require internet access**, so must be done before a shutdown occurs or during periods when it is restored. Also, don't wait until you're in a stressful situation to enact these steps; do them now, and take time to **practice using the phone** before you have to use it in a crisis.

Shutdowns often coincide with heightened information control and restrictions on freedom of expression and assembly. If you are a documenter, take extra precautions to protect yourself and your information during these periods. If there is a risk that authorities will confiscate your phone, or compel you to unlock it and reveal the contents (during a shutdown or otherwise), consider using a separate phone for documenting than your primary personal one. This can help minimize what information you are carrying that can be compromised (e.g. your contacts, accounts, messages, etc). If you are unable to use another device, you can still follow this guide to reduce the amount of sensitive data and improve security on your primary phone.

## If repurposing an older phone, wipe it first

To wipe your phone, run a Factory Reset.

Note: Studies have shown that running a Factory Reset on your phone does not necessarily wipe all the data. In fact, the only 100% secure way to wipe data is to destroy the phone, but that method isn't an option if you want to re-use the phone! In this article, an Android engineer suggests making sure the contents of your device are encrypted before the Factory Reset. Encryption is the default on most current phones anyway, but in case not, go to Settings > Security > Encrypt Phone before resetting. This way, when you factory reset the phone, the encryption key is lost, and any unerased data will be unreadable.

## Practice basic phone security

There are general phone security practices that are relevant in every situation, whether you are documenting during an internet shutdown or not. Here are some useful resources from other organizations. While nothing will guarantee 100% security, some key tips include:

- Make sure your phone is encrypted. Newer phones have encryption on by default. If you're not sure about yours, check the security settings on your phone.
- Run operating system (OS) updates regularly, as they often fix security vulnerabilities.
- Update your important apps (like messaging apps) regularly.
- Set a strong phone passcode that has at least 6 digits and does not rely on fingerprint/touch or face ID.
- Set up a screen lock and lock timer.
- Turn off location services if you don't need them (including emergency location service, location accuracy, location history, and location sharing features, and WiFi and Bluetooth scanning options). Also check location permissions for individual apps.
- Turn off Bluetooth and WiFi when you don't need them, to avoid device tracking.
- Power down the phone when you're not using it.

## Install useful documentation apps

For photo or video documentation, you can use the built-in camera app on your phone, or you can use a more specialized documentation app, like ProofMode or others, that allow for more robust metadata capture and export, identification and authentication, encryption, secure galleries, or other features.

A useful app for documenting a shutdown *itself* is OONI Probe, an open-source app that runs tests from your phone to measure whether sites or platforms are being blocked. It can show you how, when, where, and by whom sites are being blocked. Be sure to understand the potential risks before using this app.

Not sure which documentation app(s) to use? We provide some guiding questions in our tutorial, "Should I Use this Documentation App?".

## Install some everyday apps

Having very little data and only a few specialized apps on your phone may arouse suspicion. To make the device appear as if it's an everyday phone, install some everyday apps that are common in the area where you are documenting (but that are downloaded from reputable sources), and take some innocuous photos for your gallery.

For social media apps, you may wish to create and log into alternate accounts, although keep in mind that fake accounts violate the Terms of Service for most platforms, and identity verification requirements of some platforms may make it difficult to create fake accounts. In addition, you will need to spend some time creating content and adding friends to these, which can be laborious.

## Installing apps when there is no internet

Downloading and installing apps without internet access is obviously a challenge. You need to download apps in advance if you anticipate an internet outage.

One strategy that can help you and others later on is to download and save the Android Package (.apk) file for the app (**downloaded from a trusted source**, e.g. directly from the developer) on your phone storage or on a drive. Having these APKs offline allows you or others to share apps when there is no internet.

While we haven't had a chance to give this a try, the F-Droid app provides an interface to swap these APKs offline. Here is their tutorial.

## Keep real personal or private / sensitive information off the device

Try to reserve the device for doing documentation. Don't use it for email, phone calls, or messages with personal or activist contacts who could be put at risk, and do not connect this device to any of your real, primary accounts.

## Use features for obscuring content

In the event that your phone is searched, it may be helpful to make your intentions less obvious or your content harder to find. In anticipation of situations where your phone will *only be superficially and quickly examined*, you can employ simple tactics such as:

- Changing the names and icons of your app shortcuts using a Launcher app (e.g. Nova Launcher, but there are many) so it's less obvious what certain apps are.
- Using a built-in privacy feature like Private Mode (Samsung) or Content Lock (LG), if your phone supports it.
- Placing an empty file named ".nomedia" inside any folder to prevent media in a folder from appearing in your gallery. Note: If media still appears, you may need to clear your Gallery cache. This may not work consistently on all devices.

- Creating hidden folders (folders that start with a ".") using a file manager app. You can either move files to the hidden folder manually, or if you use a camera app like Open Camera, you can specify where the media you record gets stored. Make sure to turn off "show hidden files" option in your Settings so that hidden files are not visible.
- Some specialized documentation apps, like Tella or Eyewitness to Atrocities, store documentation in separate encrypted galleries whose contents are only accessible within the app, which may make it less obvious to someone searching your phone.

Documentation in these secure galleries requires a separate app passcode, so it remains encrypted even when your phone is unlocked.

## Important note about obscuring your content

It is important to note that the techniques above might be enough to throw off someone who is just quickly swiping through your phone, but **will not effectively hide your content from someone who is really looking.**

Also keep in mind that some countries may have laws that restrict or criminalize the use of security apps that encrypt or wipe your data. Using them to prevent authorities to accessing your data may be seen as destroying evidence or obstructing an investigation, and may be punishable as a crime. This map (comprehensive, but from 2017) provides a good starting place if you have questions about the laws in your country.

## Set up offline sharing

In a situation where you don't have internet after you've captured content, you may still want to get the documentation off your phone for security reasons, to free up space, or to share with others. Regularly offloading documentation from your phone will also help to minimize what information is compromised should your phone ever be confiscated and unlocked.

Even if you cannot connect to the internet, you can still connect to wifi-enabled or Bluetooth-enabled devices locally, such as another phone or a wifi USB drive. Your phone should typically come with an app / interface for you to connect and transfer. If your phone supports it, you can also plug in a USB On-The-Go (OTG) drive or connector to offload documentation to the OTG drive or another device.

These methods are discussed in more detail in our File sharing and communication during an internet shutdown tutorial and our Video As Evidence: Tech Tools – Transferring Files tipsheet.

## Practice before you're in a crisis situation

Set up the phone now if and while you have internet access. Start practicing using the apps in everyday situations (where there are no security concerns) so that you become familiar and comfortable using them. Make good basic phone security your default practice. This way the methods will be second-nature when you're in a crisis situation with other things to worry about.

*Check out the next post in this series, "Should I Use This Documentation App?"*