

Table of Contents:

[Introduction to Documenting During Internet Shutdowns](#)

[Setting Up a Phone for Offline Documentation](#)

[Should I Use this Documentation App?](#)

[Maintaining Verifiable Media During an Internet Shutdown](#)

[Backing Up Phone Media Without Internet or a Computer](#)

[File Sharing and Communication During an Internet Shutdown](#)

Introduction to Documenting During Internet Shutdowns

In June 2019, as human rights abuses and a humanitarian crisis were continuing in Myanmar, the country's Ministry of Transport and Communication [directed telecom companies](#) to shut down their mobile internet service in parts of Rakhine State and neighboring Chin State. Citing "disturbances of the peace" and "illegal activities," the Myanmar government claims to have enacted the shutdown "[for the benefit of the people](#)." In reality, the blackout cut [over a million people](#) off from access to essential information and communication, and disrupted humanitarian efforts. As Matthew Smith from [Fortify Rights](#) has [stated](#), "This shutdown is happening in a context of ongoing genocide against Rohingya and war crimes against Rakhine, and even if it were intended to target militants, it's egregiously disproportionate."

The shutdown was [partially lifted on five of the townships](#) in September 2019, but is ongoing. During the same month in neighboring Bangladesh, where many Rohingya have fled, authorities ordered mobile phone operators to [block 3G and 4G services](#) in Rohingya refugee camps and to stop selling SIM cards to Rohingya. As we enter 2020, [four townships in Rakhine](#) continue to be cut off from the world, and Bangladesh [continues to limit service](#) in the refugee camps.

Documenting During Internet Shutdowns

Globally, internet shutdowns are on the rise. According to AccessNow's [#KeepItOn campaign](#), there were 128 intentional shutdowns between January - July 2019, compared to 196 in all of 2018, and up sharply from 106 in 2017, and 75 in 2016. Around the world, governments, with the cooperation of telecom companies, are increasingly turning to internet shutdowns as a strategy to repress communities, prevent mobilization, and stop information about human rights violations from being documented and shared.

"Internet shutdowns and human rights violations go hand in hand."

- Berhan Taye, AccessNow

Shutdowns can take various forms, including [platform-specific blockages that target popular apps and sites](#), [mobile data shutdowns](#), [bandwidth throttling](#), or [total internet blackouts](#). All of these types of shutdowns are intended to disrupt the ability to communicate information and expose violations in real-time. They often occur during protests, elections, and periods of political instability, and are often accompanied by heightened state repression, military offensives, and violence. While governments may try to justify shutdowns [in the name of “public safety” or other reasons](#), shutdowns clearly take place at moments when repressive states fear losing tenuous control over their people, information, or political narrative. Shutdowns violate human rights, severely disrupt people’s [lives and livelihoods](#), and also have a global [economic impact](#).

Documenting human rights violations is as important as ever during an internet shutdown. Even if information cannot be shared in the moment, documentation can be a way to preserve voices that authorities are trying to silence, and to secure evidence of abuses that can be used to demand accountability later on. Of course, the repressive context and the technological impediments of an internet shutdown make documenting violations -- and maintaining that documentation securely -- much more challenging and risky. **How can activists capture and preserve their videos during a shutdown, and even share them offline, and do so in safer ways?**

This series

Through our work with activists who have experienced internet shutdowns, we have learned some useful tips and approaches to **capturing and preserving video documentation during internet shutdowns** that we are sharing in this series. We wrote them with Android devices in mind, but the tips can be applied to iPhones as well. Some of the strategies require advance planning (and often, internet access), so it’s a good idea to review them and implement any steps *before* you are in a situation where you do not have internet and you need to document. Save a copy of any of the tutorials so you can refer to them or share them during a shutdown. And finally, start practising the techniques and methods in your everyday work so that they become second-nature before you’re in a crisis situation.

- Prepare
 - [Setting up a phone for offline documentation](#)
- Capture
 - [Should I use this documentation app?](#)
- Maintain
 - [Maintaining verifiable media while during internet shutdowns](#)
 - [Backing up phone media without internet or a computer](#)
- Share and Communicate
 - [File sharing and communication during an internet shutdown](#)

One final note: While these tips can help you continue documenting in the face of a shutdown, we want to emphasize that the ultimate solution must be to restore internet access, and successfully defend people's [right to record](#), and freedom of expression, information, and assembly. Fortunately, there is a global movement led by organizations like [NetBlocks](#), [AccessNow](#), and many others who are actively monitoring and sharing information about shutdowns. Advocates globally are engaging in [strategic litigation against shutdowns](#). We stand in solidarity with their work to uphold human rights.

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?”](#)

Should I Use This Documentation App?

Last reviewed: 31 January 2020

There are many apps that documenters can use to capture video, ranging from your phone's native [camera app](#), to more specialized documentation apps like [ProofMode](#), [Tella](#), or [Eyewitness to Atrocities](#). Some apps have features that rely on internet access, so keep in mind that those features may not be available in the event of an internet shutdown.

We can't tell you which specific app is the most appropriate for you, since that depends on your situation, needs, and risks (check out this blog post for more on [how to assess your risks and threats](#)). With your risk assessment in hand, these guiding questions below can help you evaluate which video documentation app might work best for you.

Who made the app and do I trust them?

You should always consider the creators of any app that you download and install on your device, and whether you can trust them to not put you at risk, intentionally or unintentionally.

Some things to look out for are:

- Is the app developer reputable? What are people in your community and wider network saying about them and their tools?
- Is the app developer vulnerable? Consider their context and how likely they could be compelled to hand over your data or create a backdoor for authorities (or whether they've actually done so in the past). What country is the data stored in and what are the laws concerning court orders in that jurisdiction?
- Is the app developer maintaining the app? Unmaintained tools are susceptible to hacks that exploit discovered vulnerabilities. Check the developer's website or the app's Google Play page for the “last updated” date.
- How established is the app developer, and does it seem like they will be able to sustain the app over time?

- Is the app open-source? Apps that are open to scrutiny are more likely to have their security issues addressed or at least identified. Is the developer being transparent about the efficacy and security of the app?
- What motivations or incentives drive the app developer's work, and how might that influence their trustworthiness? For example, are they mission-driven? For-profit? Sponsored by a particular funder?
- While not a direct indicator of trustworthiness or not, the cost of the app may be an important consideration. Some apps have a high monthly subscription fee or per-video fee.

Check out the [EFF](#) surveillance self-defence guide on [choosing apps](#) for more.

Where is the app downloadable from?

You should always only download and install apps from reputable app stores or websites. Even if you have done thorough research to determine the trustworthiness of an app, sketchy app stores may misrepresent their wares and lead you to download an illegitimate imposter created for nefarious purposes. For example, last year the digital rights organization [SMEX](#) issued [a warning](#) about various websites marketing an app called "WhatsApp Plus" (to be clear, this is not a WhatsApp product!), which could potentially be saving and selling users' data, or enabling phones that install it to be hacked.

Some security-conscious developers even provide cryptographic keys that enable you to verify their authenticity. They will usually provide an explanation for how to verify these signatures.

Where will the data be stored?

Some documentation apps only store your data and documentation locally on your device, while some only or additionally send and store your data elsewhere. In many cases this is inherent to the design and purpose of the app, such as the Eyewitness to Atrocities app, which sends an unaltered copy of your documentation to a Lexis Nexis storage facility so that Eyewitness can vouch for the chain of custody and integrity of the material. You can only export your media out of the encrypted gallery within the Eyewitness app *after* it's been sent for safeguarding.

It's up to you to determine whether you need your documentation to stay on your device only, whether you need it sent and stored to a remote location that you control (as is an option with [Tella](#)), or whether to need to send it an external organization / platform that you allow to access and use your documentation. Keep in mind that during an internet shutdown, you won't be able to transmit your documentation over the internet right away, so you will need an app that at least temporarily enables you store (and ideally back up) your documentation locally (Check out [Backing up phone media without internet or a computer](#)).

If your data will be sent to a remote location, be aware of which countries the data will reside. How vulnerable is data to being exposed in those countries, whether by court orders or other means? What risks do you face by having your data exposed there?

Does the app encrypt my media?

Some apps, such as Tella and Eyewitness to Atrocities, provide file encryption and/or encrypted storage for your documentation, separate from your phone's main gallery and your phone's encryption, so that your media and metadata are never unencrypted on your device unless accessed through the app with a passcode. This means that even if your phone is unlocked, your documentation remains encrypted. This can provide an extra level of protection for your documentation.

If the app sends and stores your media to a remote location after your internet is restored, also consider whether you need your media to be encrypted while in transit and while in the remote location, as the EyeWitness app, for example, does.

Keep in mind that while encryption is legal in most places, some countries may have laws that restrict or criminalize its use. This [map](#) (comprehensive, but from 2017) provides a good starting place if you have questions about the laws in your country.

Does the app capture important metadata (without internet)?

[Metadata](#) is data that describes your video or photo, like the time and date or the location. This information is valuable for identifying, understanding, authenticating, and verifying your video or photo as documentation of a specific event. In the context of an internet shutdown, an app's ability to automatically collect certain metadata and/or to allow you to easily input useful descriptive information on the spot is especially useful, as there may be a long period of time before you can share the documentation with anyone (time during which details can be forgotten, circumstances might change, etc, etc).

Most specialized documentation apps such as ProofMode have enhanced metadata features, and gather more metadata than typical built-in camera apps. Enhanced metadata might include various sensor data, nearby wifi or bluetooth signals, device data, cryptographic hash, and user-supplied information, all which can facilitate authentication and verification of the media later on.

Keep in mind that during an internet shutdown, you will need an app that does not require data to be transmitted in order to generate or record the metadata. Some apps may rely on the internet, instead of the hardware sensors, to collect certain metadata. For example, if the location data is captured from look ups on the device, the metadata may reflect the last location where the device had data connection, instead of the actual position of the hardware. The app should also ideally allow you to store the metadata locally without internet, including saving any forms you are filling out (e.g. Tella's "offline mode").

Can I export data from the app?

Depending on your intentions for the documentation, it may be essential to be able to export the video documentation and its metadata from the app, in a format that is not proprietary to the

app; that is, to be able to open, view, and use the media and metadata outside of the app. The ability to export means that you and others are not dependent on a single app or service provider to access your documentation, and gives you more leeway in working with the content going forward. Keep in mind that some metadata may not be comprehensible if you do not have access to certain databases or conversion charts to interpret the numbers (for instance, in the case of cell tower IDs or Wi-Fi networks).

Note that some apps may have a deliberate closed chain of custody and not allow users to export, while some apps may simply not be designed with an export use case in mind. Also be aware that some apps, like Eyewitness to Atrocities, may not let you export until you have uploaded the media to a remote server (which you need internet access to do), and some apps may allow you to export the media, but not the metadata (other than any metadata that lives in the file itself).

If you need to export, ideally your app should allow you to export a copy of the media without any changes or transformations, and a copy of the metadata in a standardized readable text format. Tella metadata, for example, is stored encrypted in the Tella gallery, but can be exported as CSV. Additionally, during an internet shutdown, it is necessary to have options for exporting to offline apps or non-internet dependent services. Most apps that allow you to export have some kind of “Share” button that triggers a share menu, which Android populates with a list of apps on your phone that are capable of handling that type of content. Unfortunately app developers can customize their share menus and there is no consistency between apps.

For a larger quantity of files, it may be more efficient to access the stored files via a file manager app and copy the files from there, although you may not be able to access metadata stored in an app’s database this way. This option is also not available for apps that provide their own secure galleries, as the files will be encrypted in storage. For these apps, it is necessary to have a sharing function within the app.

Check out our comparison chart of documentation apps, and the next post in this series, [“Maintaining Verifiable Media During an Internet Shutdown.”](#)

Maintaining Verifiable Media During an Internet Shutdown

This post is part of a series on [Documenting During Internet Shutdowns](#).

Last reviewed: 31 January 2020

[Human rights defenders](#), [investigators](#), [researchers](#), and [journalists](#) often rely on first-hand documentation filmed by witnesses to monitor, report, and address human rights violations. To ensure that they are acting on correct information, these users take steps to authenticate and verify the documentation they receive, a process that can be painstaking and time-consuming.

As a documenter, there are simple things you can do to make it easier for others to verify and corroborate your documentation, so that it can be used in timely and effective ways. These few extra steps are even more valuable during an internet shutdown, considering that:

- If you can't upload right away, the publication date and location info provided by social media is not as helpful for showing that your video was filmed on or prior to a certain date or in a certain location.
- If others can't upload either, there may be less documentation available overall that can be used to corroborate your video.
- If you need to pass your video through many hands offline to get it to its destination, it may be harder for others to trace the source of the video.
- If you need to delete the original video from your phone because of heightened security or limited storage capacity with no cloud backup, or if you have to get rid of the phone, it may be harder to confirm the authenticity of the video.
- If you forget the details about a particular video and the app you're using doesn't capture / record metadata without internet access, others may not be able to identify it later.

The following tips can help you maintain your video during an internet shutdown to maximize its verifiability and usability as documentation later on.

Film or provide identifying details in the video

Try to include details in your video that make it easier for an investigator or journalist to later identify the time and place, like unique landmarks, the skyline, street signs, storefronts, license plates, flags, clocks, newspaper front pages, etc. You can also narrate basic information such as your name and contact information (if safe to do so), the time, date, and location/GPS coordinates (or write down on a piece of paper and film the paper). The more details you include, the easier it will be for someone else to research and verify the video later, even if they don't know you or where the video came from. Check out our tips on [Basic Practices for Capturing, Storing, and Sharing](#) for more.

Add description / metadata

Take advantage of one of the many specialized documentation apps that pull enhanced metadata or technical information from your phone, and allow you to manually input additional descriptive information. Keep in mind that, during a shutdown, you need an app that does not rely on internet access to record or store this metadata. Check out ["Should I Use This Documentation App?"](#) for more on how to choose an appropriate app.

Even if you're not using a specialized documentation app, you can still create supplementary information in the form of notes, maps, or photos on your phone. You can organize your video with this additional information using your favorite file manager app. The key supplementary information to include is time, date, location of the recorded incident, as well as the source of

the recording (i.e. your name and contact information) if safe to include. Export the metadata and include it with the video (you can put it all in a folder and zip it) when you share it.

Keep a backup

Back up media from your phone regularly, ideally to 2 separate storage devices. You can, for example, connect On-the-Go (OTG) or wireless thumb drives to your phone, even without a computer. Check out our tips on [“Backing up phone media without internet or a computer”](#) for more details. Backing up will ensure you retain a copy of your video in case you lose or break your phone, or you need to delete videos from your phone. Having a secure copy of your original video also enables an investigator or journalist who sees your video through some other means to get the video directly from you later (as long as they are able to trace it back to you), creating a shorter and more complete chain of custody.

Check out the next post in this series, [“Backing Up Phone Media Without Internet or a Computer.”](#)

Backing Up Phone Media Without Internet or a Computer

This post is part of a series on [Documenting During Internet Shutdowns](#).

Last reviewed: 31 January 2020

[Backup](#) is key to ensuring your data and documentation are not accidentally deleted, corrupted, or lost if your device is confiscated. During an internet shutdown or slowdown, you might not be able to run your regular cloud backup or send your documentation to a safe offsite location. Offloading to a desktop or laptop is one way to back up, but since people often do not have access to a computer, here are some options and tips for backing up your media from your phone during an internet shutdown without one.

Use an OTG or wireless drive

OTG, or on-the-go, drives are a type of USB drive compatible with many (but not all) Androids. You can plug an OTG thumb drive directly into your phone, or use a OTG-to-USB adapter to connect your phone with a regular USB hard drive. With OTG, your phone provides the power for the drive.

Popular brands of OTG drives include SanDisk, Kingston, and Samsung, although there are many others. They typically cost between US\$8-\$25 depending on the storage capacity.

Wireless thumb drives / hard drives are similar to regular hard drives except that they do not require cables. This allows you to connect devices that don't normally connect to hard drives, such as your phone. An advantage of a wireless drive over an OTG drive is that you can connect multiple users to the same wireless drive at once. This can be useful, for example, in a protest situation when you are filming as a team -- everyone's footage can be backed up to a hard drive that another team member is carrying. Note that because they are not drawing power from a device, wireless drives rely on battery power and need to be charged.

SanDisk is probably the most popular brand of wireless thumb drives, although there are others. Wireless thumb drives are generally more expensive than OTG drives, and range from about US\$25-\$100 depending on the storage capacity. Larger wireless external hard drives start at around US\$150 depending on the storage capacity.

Alternative: Use an old unused phone

If you don't have an OTG or wireless drive, but you have an old phone that still works that you no longer use, you can also re-purpose it for backup. As long as both phones are in physical range, you can connect and copy media from one to the other using Bluetooth, WiFi Direct, or Near Field Communication (NFC) / Android Beam. Bluetooth and Wifi Direct are both wireless technologies that can "pair" two devices without another router or access point in between. WiFi Direct provides a wider range and faster data transfer than Bluetooth, but uses up a lot more power. Meanwhile, NFC has a much shorter range (~4cm) and much slower transfer speeds than either Bluetooth or WiFi Direct, but connects faster and uses less power, so can be useful for quick small transfers when you have both devices in hand.

Your phone probably has built-in Bluetooth, WiFi Direct, or NFC apps / features that allow you to choose nearby devices to share with. If both phones have Files By Google installed, you can also share files offline using these technologies within the app.

Important: the downside to the ease of connection provided by these services is that they are not secure. Bluetooth and wifi beacons/scanners can be used to trace your location or probe your device for information. Infiltrators may try to pair with your device, send you unwanted files, or even gain control of your device if it is vulnerable. **To be safer, turn these services off when you are not using them and only turn them on when you're in safe locales, limit app permissions to only what/who you need, and practice good phone security like running updates and having a strong passcode.**

Include any separate description / metadata

When copying media to an OTG drive, wireless drive, or an old phone, it is useful to include any descriptive information or metadata that may be separate from the media. Many [documentation apps](#), for example, generate CSV or JSON text documents that include metadata pulled from

the device (e.g. geolocation, time, date) and any description manually inputted by the user. Make sure to export and include these metadata documents in your backups too.

Password protect the drive

Many wireless drives can be password-protected with a mobile app that comes with the drive. Note that password-protection is not the same as encryption (see below). Most wireless or OTG drives do not enable full-disk encryption using only a mobile phone, although they may be full-disk encrypted using a computer.

Consider encrypting the files

If you need to store your files more securely, you might consider encrypting your backups. While you may not be able to encrypt most wireless or OTG drives with a mobile phone, you can encrypt the files themselves before you move them onto the drive. Some apps that can encrypt files on Android include [ZArchiver](#), and [RAR](#). Be aware that you must remember your encryption passwords. There is no way to recover encrypted files if you lose the password.

Keep in mind that some countries may have laws that restrict or criminalize the use of encryption. 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 [2017 map](#) may be outdated but provides a good starting place if you have questions about the laws in your country.

Make 2 backups in separate locations

A single backup is not always reliable. For example, you might lose the backup device, damage it, or it might just randomly fail. IT experts usually advise people to have 2 backups (i.e. 3 copies total), on separate devices kept in separate locations. This helps mitigate the variety of risks to any one particular copy.

Check out the final post in this series, [“File Sharing and Communication During an Internet Shutdown.”](#)

File Sharing and Communication During an Internet Shutdown

This post is part of a series on [Documenting During Internet Shutdowns](#).

Last reviewed: 31 January 2020

The ongoing internet shutdown and crackdown in Kashmir, the longest internet shutdown ever imposed in a democracy, has had a [catastrophic impact](#) on the lives of people in the region. Adding insult to injury, in December 2019, Kashmiris' [WhatsApp accounts started being revoked](#) due to users' 120 days of inactivity as per WhatsApp policies.

At the time of this writing in January 2020, the Indian Supreme Court ruled that the indefinite shutdown in Kashmir is [illegal and an abuse of power](#). Limited broadband and mobile internet has been restored in some areas, but only to select “whitelisted” websites.

Internet shutdowns are designed to block people from sharing information and communicating (and also push people into less secure forms of communication such as mobile phone and SMS, which are easier for authorities to intercept and monitor). There are not always good workarounds during complete shutdowns. During the strictest periods of the shutdown in Kashmir, for example, people resorted to [using handwritten notes and couriers](#) to get messages to their loved ones.

We don't have sure-fire ways to circumvent all blockages, but through conversations with activists and peers, we have learned some methods and approaches for offline sharing and communication that may work for you, depending on the circumstances. Note that some of these options require internet to initially set up (e.g. to download apps, etc).

Share files directly with Bluetooth, Wifi Direct, or NFC

You don't need to have an internet connection to connect your phone with another nearby device via Bluetooth, Wifi Direct, or Near Field Communication (NFC) (sometimes called Android Beam on older devices). Bluetooth and Wifi Direct are both wireless technologies that can “pair” two devices without another router or access point in between. WiFi Direct provides a wider range and faster data transfer than Bluetooth, but uses up a lot more power. Meanwhile, NFC has a much shorter range (~4cm) and much slower transfer speeds than either Bluetooth or WiFi Direct, but connects faster and uses less power, so can be useful for small transfers when have both devices in your hands.

You likely have Bluetooth, WiFi Direct, and NFC features built into your phone that show up in your sharing options. In addition, apps with file sharing features, like [Files By Google](#), also integrate these technologies.

Important: the downside to the ease of connection provided by these services is that they are not secure. Bluetooth and wifi beacons/scanners can be used to trace your location or probe your device for information. Infiltrators may try to pair with your device, send you unwanted files, or even gain control of your device if it is vulnerable. **To be safer, turn these services off when you are not using them and only turn them on when you're in safe locales, limit app permissions to only what/who you need, and practice good phone security like running updates and having a strong passcode.**

Share files with a wireless drive or via a Wireless Local Area Network (WLAN)

A wireless hard drive or flash drive can be used to share files among a team, or multiple people at one time. The wifi drive will typically come with instructions and/or an app for connecting your phone to the drive, and is relatively easy to use. Remember to set a password on the drive for security.

If you don't have a wireless drive, you can also share files on a regular USB drive by plugging it into a wireless router. A travel router with a USB port, for example, is relatively inexpensive and very portable. Users can connect to the USB drive through a local network (no internet required). To access files on the connected USB drive on your phone, you will need to use a file manager app that can connect to networked storage, such as [Solid Explorer](#). The IP address of your router can usually be found in your phone's advanced wifi settings.

Meanwhile, another option is [PirateBox](#), a do-it-yourself project that provides freely licensed software. Users can share files as above, but Piratebox lets them do so anonymously, and also includes chat and messaging features. Setting up a Piratebox requires downloading, installing, and setting up a few pieces of software. [Instructions](#) are on the Piratebox website.

Update: the Pirate Box project is [slowly closing](#). The website and github repository are still online, but the main developer of the project is no longer actively maintaining it.

Communicate via peer-to-peer chat

Two new-ish peer-to-peer messaging apps that we have become aware of through activist networks are [Briar](#) and [Bridgefy](#). We haven't tried them yet, but we know others who are testing them.

[Briar](#) is an open-source, end-to-end encrypted messaging app that doesn't rely on a central server, but instead syncs messages between users' devices (so content lives on each user's device). It can sync even when there is no internet using Bluetooth or WiFi (when there is internet, the app syncs devices over the [Tor](#) network). Briar also features private groups, public forums, and blogs. When using offline, your range is limited by your Bluetooth or WiFi range (maximum ~ 100 meters).

Meanwhile, [Bridgefy](#) is an end-to-end encrypted (except when using "broadcast" feature) messaging app that uses Bluetooth to send messages. Unlike Briar, messages can travel longer distances by hopping along a mesh network of other Bridgefy users (only the intended recipient can read the message). Bridgefy lacks Briar's private groups, forums, and blog features, but it does have a Broadcast mode through which you can send a message to up to 7 Bridgefy users within range, who do not need to be your contacts (Broadcast messages are by necessity not encrypted).

Communicate via encrypted SMS

SMS text messages are sent over cell networks and do not rely on the internet, so may still work during internet shutdowns. However, SMS is considered very insecure. Unlike internet-dependent apps like WhatsApp or Signal, SMS is not end-to-end encrypted. This means that text messages (and their metadata) can be read by governments and mobile carriers, or intercepted by hackers. SMS can also be “spoofed,” meaning that a sender can manipulate their address information to impersonate another user.

If you need to use SMS, [Silence](#) is an app that end-to-end encrypts SMS messages. It is open-source and uses the Signal encryption protocol. While we haven’t tried it ourselves, we have heard that others have used it. Both the sender and recipient need to have it installed and exchange keys with each other. Since SMS messages necessarily go through your telecom’s servers, even with Silence the fact that you are sending an encrypted message and the metadata about your message will be accessible to the telecom company.

Partial shutdowns: Circumvent blocked sites

An “internet shutdown” often does not mean total internet blackout, but rather blocking access to specific websites or social media platforms. Governments, via internet service providers (ISPs), can block sites based on IP address, content, or via DNS lookups. Unsure if a site is being blocked? Organizations like [Open Observatory of Network Interference](#) and [Netblocks](#) monitor and measure internet disruptions and censorship around the world.

Fortunately, as long as you have internet access, there are some ways to try to get around the partial blocks. As with encryption, keep in mind that circumventing blocked sites may be criminalized in your country.

VPN

One way to bypass IP-based and content-based blocking is to use a virtual private network or VPN, such as [ProtonVPN](#) or [TunnelBear](#). When you connect through a VPN, your internet traffic is encrypted and routed through a VPN server in another location, such as in another country, thus concealing the true destination and the content of your traffic to your ISP.

Keep in mind that some governments ban VPN usage or may try to detect and block VPN connections. It is also important to use a trustworthy VPN provider, and preferably one that does not store data or logs, since the provider will be able to see your internet activity. Be aware of what country the VPN provider is based in, and what legal processes they may be subject to based on their jurisdiction. Also consider that government-approved VPNs may actually enable surveillance and inspection of your data.

DNS servers

DNS (“domain name system”) servers work by translating the domain names or URLs that a user types into a browser into the numerical IP addresses that the internet uses to identify webpages. An ISP can modify the DNS servers it controls to block certain queries, or to return an incorrect page saying that the website doesn’t exist. In 2014, Turkish Prime Minister Recep Tayyip Erdoğan [attempted to block Twitter](#) during Turkish elections using this technique. The ban was [quickly thwarted](#) by activists who shared step-by-step tips on how to use VPNs and change DNS servers.

You can change the default DNS server in your phone’s network or wifi settings. Instead of the default DNS server, you can use alternative DNS servers such as [Google Public DNS](#) or [CloudFlare](#) to get around DNS-based blocks. Cloudflare also has an app called [1.1.1.1](#) that allows users to switch to a Cloudflare DNS server through a simple app interface.

These are just two ways to circumvent the most common blocking techniques. Check out helpful guides from [Internet Society](#), [Access Now](#), [Security-in-a-Box](#), and [EFF](#) for more in-depth information.
