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.