How to communicate and document human rights violations during an internet shutdown

NOVEMBER 16, 2020 | BY LIKHITA BANERJI

Amnesty International investigation 'A web of impunity: The killings Iran's internet shutdown hid' is the latest addition to a mounting pile of evidence highlighting a disturbing trend– hiding human rights violations through internet shutdowns. This tactic is fast becoming a favourite of rights-violating governments around the world.

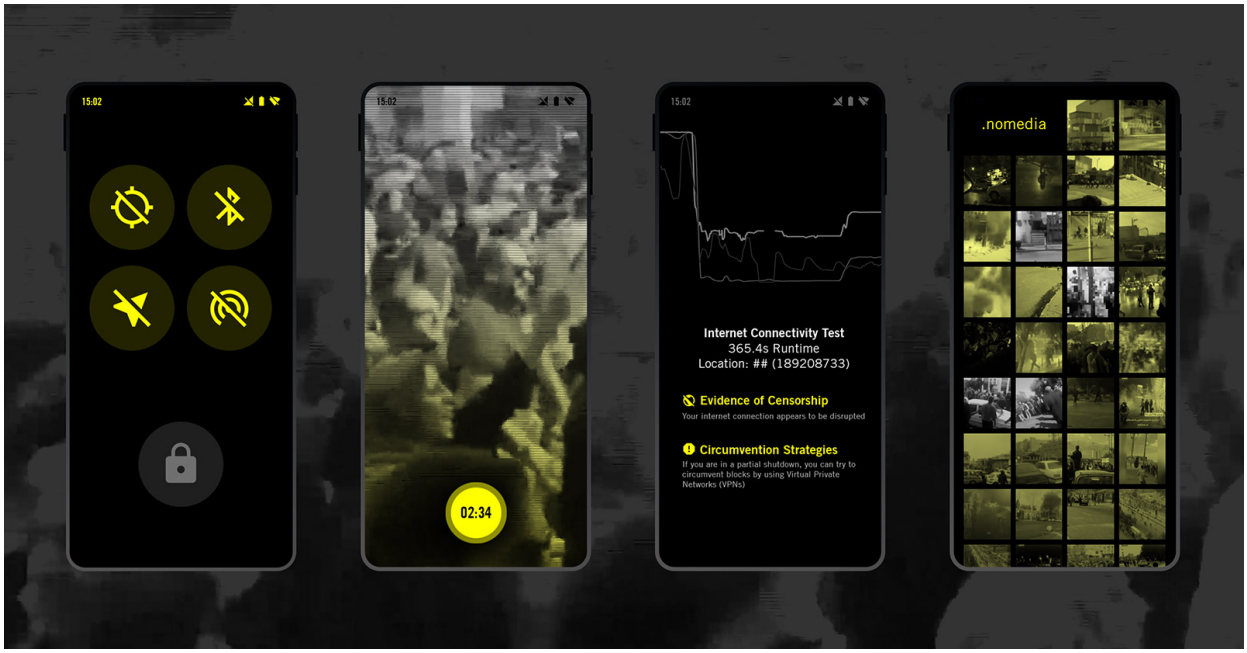
As anti-establishment protests swept across Iran in November 2019, authorities imposed an internet shutdown. Amnesty's investigation reveals that within the first 48 hours of the shutdown, security forces killed more than 220 people. With millions of people cut off from the global internet, the absence of information sharing significantly impeded the truth from coming out. It took Amnesty's investigators thousands of hours of relentless fact-finding to record and verify the deaths of 304 people. We believe many more were killed.

For activists, journalists and researchers, having the ability to document evidence and safely communicate during an internet shutdown may be key to shining a light on grave human rights violations and for holding those responsible accountable.

Open source researchers and digital security experts have successfully tried ways that activists, journalists or researchers can gather, store, and even share evidence during an internet shutdown. This guide outlines steps you can take *before* and *during* an internet shutdown to safely communicate and document critical evidence of human rights violations.

Preparing to document before a shutdown

Before documenting sensitive human rights information on your device, you should ensure that you have practiced the basics of digital security. Before a shutdown, there are several



Open source researchers and digital security experts have successfully tried ways that activists, journalists or researchers can gather, store, and even share evidence during an internet shutdown.

Practice basic digital security on your mobile device

steps you can take to make your smartphone more secure. **It is, however, important to note than there is no such thing as complete security, and you should carefully evaluate your risk.**

At a minimum, you should ensure that all your mobile devices are encrypted. You should also ensure that you update your operating system and apps regularly. You should use a strong passcode or passphrase, and avoid relying on finger-print or facial ID to unlock the device. Disable Bluetooth, WiFi, and location services when they are not in use, for example by enabling the Airplane Mode.

Digital security experts have developed guides that provide detailed and advanced information on securing your mobile devices. You can learn more by reading further.

https://ssd.eff.org/en/module/problem-mobile-phones

https://www.securityplanner.org/#/all-recommendations

Securely back-up your data

In a high-risk, fast-evolving environment, your devices can be seized by authorities, or can be lost. While backing up your data during a shutdown may prove to be challenging, you should secure all your data on your devices *before* any possible shutdown. Back up all your devices to an external hard drive or to a cloud service. Practice using password managers and 2-factor authentication.

Use tools to obscure content on phones

When using your phone to document evidence at protests or in other high-risk situations, there is a chance that you may be stopped, and your devices searched. In such an event, the human rights organization WITNESS recommends simple steps to obscure content on your phone. These tips will only work if a mobile device is superficially examined and should not be relied upon if more sophisticated examination tools are used. In addition, you should check if using these tools may pose additional risks to your context – for example, if the use of such apps is criminalized by local law.

- WITNESS recommends using tools to change the names and icons of your apps through Launcher applications such as Nova Launcher. This makes it not immediately easy to recognize which apps are on the device. This is possible on Android phones.
- For some older phones that may have dated Android systems, you can use built-in features that can allow you to hide content on your phones (such as Private Mode on Samsung devices).
- You can also enable 2-factor authentication through passcodes for specific apps like WhatsApp, Signal, Firefox, and Wire on both Android and iPhones.
- For Android phones, WITNESS further recommends placing an empty file named ".nomedia" inside any folder to prevent media in a folder from appearing in your gallery. Creating hidden folders (folders that start with a ".") using a file manager app will also work.
- You could also use specialized documentation apps, such as Tella or Eyewitness to Atrocities, which store documentation in separate encrypted galleries and make content are only accessible within the app. This makes it harder to find content if your phone is searched.
- Use encrypted applications such as Signal, and use 'disappearing messages' functions to automatically erase sensitive communications on both ends of a conversation

Download apps to circumvent censorship

If you are in a partial shutdown, you can try to circumvent blocks by using Virtual Private Networks (VPNs). You may then be able to access regular communication channels such as email or encrypted applications to safely share any evidence of violations that you may have collected.

To enable you to do this, you should download VPN applications or browser extensions before a shutdown. Avoid free VPN applications, and instead use a paid application from known companies.

Please note that VPNs may be criminalized in some contexts or may invite backlash from authorities even where they are not expressly forbidden. Please assess the risk in your specific context before downloading and using VPNs.

Documenting During a Shutdown

Navigate censorship or partial blocks

If you think you are experiencing an internet shutdown, you should check to see if some services work. Shutdowns can take many forms. Authorities may try to throttle speeds, block certain websites, ask internet service providers (ISPs) to shut down, or sometimes block off the internet entirely. You can try to test what is accessible to ascertain what kind of network disruption you may be experiencing.

You can also use VPNs or try to switch your DNS Server to circumvent blocks. The encrypted communications app Signal has a 'censorship circumvention' feature which can be turned on when the application may be blocked.

Documenting evidence of violations

Documenting evidence of human rights violations can make you a target yourself or, in some cases, even violate domestic law. Therefore, any documentation should be undertaken whilst prioritising your safety and the safety of those around you. If you decide that it is safe to document, then you should document with verification in mind. Film the area around you to make it easy for a third party to geolocate where the violation happened. You can also narrate the time and location of events and describe what you are seeing. Film major landmarks or street signs where possible and safe. Try and take slow panning shots of the area. If, during your documentation process, you come across ammunition, tear gas canisters or other munitions, avoid touching them as they could be dangerous.

Documenting evidence of the shutdown itself

An internet shutdown that tries to hide evidence of state repression is a human rights violation in and of itself. Evidence of a shutdown can and should be preserved. If you can have detected a shutdown, you can also share technical and other evidence of this with the Keep It On coalition– a global network, which Amnesty International is a part of, leading the fight against internet shutdowns. You can do this by sharing screenshots of blocked websites or recording your own experience of experiencing a shutdown.

The OONI Probe app, can help measure censorship, throttling, and shutdowns. However, in some contexts having the app installed may pose specific risks and invite backlash from authorities. Before installing this app, you should conduct a thorough assessment of whether this may be too risky in your context. You can do this by reading OONI's summary of potential risks.

If you anticipate a shutdown, you can also contact digital rights groups within your country who may document shutdowns and provide support. For instance, SFLC.in in India documents network disruptions.

Communicating and sharing media during an internet shutdown

You can share media and other files with your trusted contacts who are physically proximate to you using Bluetooth or Near Field Communication (such as Android Beam or iOS Airdrop) tools on your device. Read WITNESS's guide on detailed instructions on file-sharing, and our own guide on how to share photographs and videos via WhatsApp while preserving metadata.

For organising and communicating otherwise, you can use a host of apps that rely on peer-to-peer communication. They often work with a slight delay and work better if a large number of people are using them. Examples of such end-to-end encrypted apps are Bridgefy and Briar.

Despite efforts, if you have collected evidence that you cannot upload or send straightaway, ensure that back up any evidence in an external hard disk that you may be able to share when you are back online. You should encrypt your external drive. This may be key to ensuring that evidence of grave violations sees the light of the day.

Ultimately, it is important to note that documenting violations during an internet shutdown is risky. You should prioritise your personal safety and well-being, and make informed decisions about your risk levels before documenting evidence.