Keeping the Internet accessible in Sudan, South Sudan and the Democratic Republic of Congo through circumvention tools in the event of a shutdown

An Open Technology Fund funded Campaign

Internet shutdowns, carried out for stifling communications amongst protesters and dissenters, have become increasingly common in African countries during key political events, especially election periods. For example, in December 2016, both the Gambia and the Democratic Republic of Congo (DRC) shutdown the Internet despite strong statements from the Keep It On campaign and other parties. Further, there was an anticipated escalation of internet censorship events and possible shutdown in Sudan and South Sudan on December 19th, following similar shutdowns in Sudan 2013. Although the shutdown did not materialise in both countries, there are fears of such events occurring in future given the recent civilian protest in November 2016 as millions of Sudanese protested the government's economic policies and challenged its legitimacy. There are also similar fears of a repeat in the DRC unless the country finds a durable political settlement.

In light of the above, we are teaming with organisations and individuals, some of whom are listed below, to raise awareness of circumvention tools and related projects supported by the Open Technology Fund to help people in Sudan, South Sudan and the Congo to circumvent future internet shutdowns and help keep the internet accessible in these countries under those circumstances. This campaign builds and largely benefits from a similar Access Now campaign on the DRC on 19 December 2016.

The list of tools and projects begins with basic recommendations and then provides more complex solutions that apply in different scenarios.

Remember: this is general advice, and it may not fit your particular circumstances. For further support, you can contact the individuals and organisations listed in the document.

In addition, as we note below, in some countries using Virtual Private Networks (VPNs) or other circumvention tools may be illegal.

Ways to circumvent shutdowns

1. Browse the Internet securely

Use HTTPS
This is the secure version of the HTTP protocol used to access websites, and sometimes the encrypted version of a website may not be blocked.

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that ensures you visit the encrypted version of a website, whenever such version is available.

- Website: **https://www.eff.org/https-everywhere**.

Are all versions of the website blocked?
Check if both mobile and regular websites are blocked. For example, you can visit **http://twitter.com** and **http://m.twitter.com**, the mobile version of Twitter. Censors that block websites or web pages usually work from a blacklist of banned websites, so you can use anything not on that blacklist.

2. Circumvention Tools

Web-based proxy tools
Web-based proxy tools can help circumvent censorship. Basically, the users route their HTTP requests through a different computer (the proxy).

Note: web-proxy users must be careful, since there are bad proxy servers capable of rerouting and modifying requests for malicious purposes. Never use or trust a proxy server that no one has ever heard of. And even if you receive the proxy from a trusted partner, play it safe and do not pass on any private information, especially if it is not encrypted.

Website: **http://proxy.org/**

Psiphon is an award winning circumvention system that uses a combination of secure communication and obfuscation technologies.
Compatible with Android 2.2 and up.
Works on Windows Vista, Windows 7, and Windows 8 (desktop).
Website: http://www.psiphon3.com
User guide: **http://www.psiphon3.net/en/user-guide.html**

Lantern is an open-source software application for desktop and mobile n internet proxy tool designed to provide you with access to the open internet. Lantern is unique because it uses peered connections as a source of internet connectivity when servers are unavailable.
Available for Android, Mac, Windows, and Linux. (Desktop).
Website: https://getlantern.org/

3. Virtual Private Networks

A VPN creates an encrypted tunnel between your device and a server somewhere else in the Internet. All of your traffic is then routed through this tunnel, protecting you from adversaries that might want to tamper or block your traffic in the way. Although your traffic will be encrypted, the VPN provider can keep logs and records of your online activities, therefore it is important to trust the VPN provider you use. **This site** compares many different VPN providers and can be useful when selecting a VPN provider.

Bitmask is a client-side VPN that uses Riseup and Calyx VPN servers. Available only for Android and Linux users. Windows and Mac versions are expected to be released soon.

IMPORTANT NOTE: In certain countries, using VPNs or other circumvention tools may be illegal.

Tor Browser is an open-source software that protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world. This makes your communications difficult to trace, but also allows you to bypass online blocks.

At certain locations, where connections are slow, it might be difficult to establish a connection through the Tor network.

The Tor Browser Bundle lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive.
Website: https://www.torproject.org

Please keep in mind that only the traffic from the Tor browser will go through an encrypted an anonymous channel. Other applications, like Skype or a regular browser, will not be routed through the Tor network, even if the Tor browser is running.

If Torproject.org blocked
If torproject.org is blocked, download Tor Browser with gettor: https://github.com/TheTorProject/gettor

If the Tor network is blocked, get Tor bridges (https://bridges.torproject.org/) to circumvent the blocking and connect to it.

If WhatsApp and/or other mobile apps are blocked, Android users can use the VPN mode of Orbot (https://www.torproject.org/docs/android.html.en) to access those apps over the Tor network. **Orbot** is an anonymity tool for mobile devices. The most recent versions of Orbot allow users to redirect all the traffic of their apps through the Tor network, using a Virtual Private Network (VPN) on Android through the touch of a button.

Orbot is only available for Android.
Website: https://guardianproject.info/apps/orbot/

Below are Hands-on guides on how to install and use Tor Browser (and bridges):

- Windows: https://securityinabox.org/en/guide/torbrowser/windows
- macOS: https://securityinabox.org/en/guide/torbrowser/os-x
- Linux: https://securityinabox.org/en/guide/torbrowser/linux

If there isn't a total internet shutdown and only certain services are blocked, users can find alternative (and more secure) communications tools through this resource: https://myshadow.org/resources

FreeBrowser
FreeBrowser provides a way around censorship but it will not work if internet is shutdown.
Website: https://freebrowser.org/en/

The app works for Android only and is a normal browser app with circumvention built into it.

Tails is a live operating system that you can start on almost any computer from a DVD, USB stick, or SD card. Tails uses the tor network to route your communications, and includes several tools that help you protecting your privacy and anonymity. Because of the default usage of the tor network for your Internet traffic, tails will be useful to circumvent online censorship.

- Website: **https://tails.boum.org/**

Interactive Guide: **https://tails.boum.org/install/index.en.html** (en Français: **https://tails.boum.org/install/index.fr.html**)

4. Umbrella App for Security Management
For security management, you mind find Umbrella App useful. It has guides on digital and physical security topics ranging from sending a secure email to dealing with a kidnap:
https://play.google.com/store/apps/details?id=org.secfirst.umbrella
More information here:
www.secfirst.org
Download Umbrella App on Android from:

- Google Play Store: https://play.google.com/store/apps/details?id=org.secfirst.umbrella
- Amazon App Store: https://www.amazon.com/Security-First-Umbrella-made-easy/dp/B01AKN9M1Y
- F-Droid Repo: https://secfirst.org/fdroid/repo
- F-Droid Fingerprint: 39EB57052F8D684514176819D1645F6A0A7BD943DBC31AB101949006AC0BC228
- Github Repo: https://github.com/securityfirst

About the Project

The project is being undertaken by Arthur Gwagwa: A Senior Research Fellow in the Centre for Intellectual Property and Information Technology Law, Strathmore University under the Open Technology Fund Rapid Response Fund, either in collaboration or the support of the following organisations and individuals:

- **Access Now**

You may also get further direct support from Access Now helpline if you need it. Here's how to contact Access Now.

- **Localisation Lab**

Localises training material in local languages. Here you can find all the projects, some 60 different circumvention, encryption, privacy, transparency tools and training materials. You

can also look up by language what they have already available. They have very active teams in most languages. Contact: dragana.kaurin@localizationlab.org

- **Tor project**

They have created a few animations and tutorials explaining how to use Pluggable Transports with Tor Browser. These materials are really helpful for training or when explaining those to users.
If you need any help explaining Tor Browser and/or PTs Isabela would be happy to help.
Contact: isabela@torproject.org

- **The Guardian Project**

- **Security First**

Contact: Rory Byrne
rory@secfirst.org

- **ASL19**

Have done similar work in the Middle East including in Arab speaking countries
Contact: sina@asl19.org

- FreeBrowser

For explanation on how it works, contact: charlie.smith@greatfire.org

- **Frontline Defenders**

They work with Human Rights Defenders on the Frontline.
Contact Digital consultant for Frontline Defenders in the Sub-Saharan region: ronald@frontlinedefenders.org

- Internet Sans Frontières

Internet Sans Frontières is not for profit organization, which defends an open and free Internet.
Contact: Julie Owono: julie@internetsansfrontieres.org