Censorship Circumvention

When experiencing any form of censorship – from the blocking of specific websites and apps, to the intentional slowdown of speeds across the network, to full shutdown events - understanding how to continue your work and maintain communications can be a daunting task. This section outlines some of the tools you can use to prepare for censorship and network disruptions, monitor and document network disturbances, guides to help you and your organization stay connected event during a shutdown, and tips for how to bypass censorship to get your message out even during a crisis.

Introduction to censorship and circumvention

What does censorship look like? And what can you do about it? Before diving into the specific tools and best practices, it is important to first answer these fundamental questions. The following resources are useful starting points for anyone looking to learn more about censorship and circumvention.

- The Electronic Frontier Foundation produced a useful primer called **'Understanding and Circumventing Network Censorship'** that introduces the concept of censorship and what is means to circumvent network disruptions. This is helpful as a starting point for getting to know more about what shutdowns are and how you might begin to respond.
- In **A Taxonomy of Shutdowns** Access Now scrutinizes eight internet shutdown types to help technologists and digital help desk practitioners better understand, prepare for, circumvent, and document the shutdown of networks.

Preparing yourself and your team for a shutdown

The following resources provide guidance and tips for how you can prepare for a network disruption. This includes some useful compilations of tools, as well as step by step guides.

- **Digital Safety Tips for Network Disruptions** outlines some basic steps to prepare for and navigate internet shutdowns: from understanding shutdown types, to using VPNs and establishing communications, to documenting network disruptions.
- **How To Bypass Internet Shutdowns:** This guide and associated toolkit provide another clear and not heavily technical approach to bypassing internet shutdowns. It includes a useful introduction to shutdowns (based largely on Access Now's annual report) then dives into the specific steps one can take to connect even during a blackout.

- Responding directly to the request for easy to share information about circumvention tools during a shutdown, Localization Lab created '**Ethiopian Resources for Open Access and Digital Safety'**, short GIFs in 4 languages and a video illustrating how to download and use a VPN when you are no longer able to use messaging applications or access content online. They aggregated a number of additional digital security and safety resources and outreach materials localized into Amharic, Oromo, Somali and Tigrinya, available on one easy-to-access page on the Localization Lab site here.

So, how do I actually circumvent censorship?

There are a plethora of tools, software, and other services that help you get around specific forms of censorship. This section introduces a handful of useful curated lists of tools for different user profiles.

- **Quick Guide to Circumvention Tools:** Internews developed this primer that offers an overview of many of the most effective circumvention tools you can use to connect during a shutdown.
- **Choosing the VPN that's right for you:** As a part of EFF's Surveillance Self Defense playbook, this guide walks through best practices and recommendations for selecting which VPN is best for you.
- **Lawyer's Hub "user-friendly primer:** Lawyers Hub Kenya built this user-friendly primer that provides an easy-to-read introduction to shutdown advocacy, including definitions of shutdowns, network measurement tools, censorship circumvention methods and other useful information for understanding and responding to shutdowns before they occur.
- **Internet Shutdowns and medical practitioners/patients:** This guide, developed by Prince Madziwa with funding from Internews introduces how medical practitioners and patients can utilize available tools to communicate about medical services or needs during partial or complete internet shutdowns.

Connecting during a shutdown: the tools

In addition to the tools included in the guides outlined in the previous section, you can also find some OPTIMA recommended tools, including VPNs and secure offline messaging apps, here.

- **Shutdown Communications Methodologies**: This quickguide introduces Briar and Bridgefy, two tools that can be used to communicate during a shutdown using SMS and Bluetooth technologies. This guide offers a clear description of concrete steps advocates can take to immediately restore connections even when network fail.
- **How to Send and Receive Apps Offline:** F-Droid allows users to share certain applications even when the Internet has been shut down. This resource outlines how and when to use F-Droid as a tool to bolster communications and advocacy efforts during a crisis.
- **Second Wind:** Developed by the Guardian Project, Second Wind is way to share applications while offline to assist in information distribution, navigation, documentation and more.

- **Psiphon:** Psiphon is a tool that allows users to send and receive data through a secure network while also disguising the type of traffic being transmitted and even where it is coming from. Psiphon technology is designed to be resilient to censorship, including attempts to interfere with Psiphon network traffic directly.
- **Tor Browser:** Tor, a common VPN used by many human rights defenders around the world, developed this introduction to pluggable transports, tools that can be used to bypass even censorship of traditional circumvention apps.