Pre-election Internet Shutdown Preparations Checklist

While this checklist is best used before an election that could trigger an internet shutdown (because it is a clear date to plan around), you can use it to prepare before any event. If shutdowns are common in your region or country, you should also try to have all of these things in place as soon as possible.

Please note that depending on the political situation, this checklist should be combined with a digital and physical security checklist:

Do we have a key contact info sheet (including telephone, signal, relevant social media, secure location if needed) for:

- The core members of our coalition
- Important journalists/media contacts
- Designated partners in key geographic regions trained to collect network data before, during and after a shutdown (see network measurement plan)
- Lawyers who can be consulted for legal questions
- International advocacy and support organizations (Access Now help desk, OONI, etc)
- Communities we support that might need assistance (at risk activists, vulnerable communities)

Do we have a communications plan established with our core anti-shutdown coalition members so that we can communicate/ coordinate no matter what the censorship scenario is?

- Have you circulated a list of verified and secure circumvention tools that coalition members can use in case of blocking of social media platforms?
- Have you established a contact out of the country who can share content and securely operate social media accounts should access be denied within the country?
- Do you know SMS/phone numbers of key contacts to coordinate around network measurement, campaigns & support should internet services be disabled? **note that SMA/voice is easier to surveille, see applications below that make SMS more secure*
- If all forms of communication are disabled, do you have a secure location (or set of locations) designated for people to physically meet?
- Have you downloaded key applications to phone and desktop in advance? These can include:
    - Your choice VPN or circumvention tool* *(note the risks of using VPNs in certain countries)*.

    - At least one backup VPN in case of blocking. This could include a self-hosted optionlike outline or algo which is less likely to be blocked. *(requires some technical ability)*
    - Peer to peer messaging apps like Briar, Bridgefy, or Firechat (refer to circumvention guide for more details on the uses and security tradeoffs of these applications)
    - Network measurement applications such as OONI & NDT speed test
- Other forms of communication you can seek access to:
    - International sim cards
    - Satellite services
    - Mesh networks
    - Offline security & app-sharing software like F-Droid and Veracrypt
    - Applications that make SMS more secure like silence.im or frontlinelocal

Do we have a network measurement plan? This plan should include

- Designated & trained people in diverse areas of the country prepared to run tests to test variable geographic access and to test different networks (different ISPs & broadband/mobile connections)
- A distributed measurement worksheet for logging measurements in a systematic & coordinated way. Make sure everyone has
    - Downloaded OONI Probe (on phone and PC) & turn on automatic collection of measurements.
    - Is prepared to run mlab's NDT test to track performance before, during, and after a shutdown
    - Is prepared to use software like IODA dashboard to track outages OR (better) hardware like RIPE atlas probes to track outages
- Contact information for network measurement experts in country
- Contact information for network measurement experts and organizations like OONI, MLab, and IODA out of country
- An explainer sheet about network measurements that can be circulated along with measurements after a shutdown to key journalists, lawyers, and activists

Do we have a legal plan?

- Do you have lawyers who understand legal justifications for shutdowns
- Do you have a legal explainer ready to be modified to circulate before, during and after a shutdown?
- Do you have people in key areas prepared to collect technical evidence as well as to document the social/economic impact of shutdowns for post-event legal action?

Do we have our campaign timeline?

For before a shutdown:

- Do we have a plan to circulate key information in the days before a possible shutdown with the goal to PREVENT the shutdown?
- Do we have copy ready to go out to journalists and other stakeholders on how internet shutdowns violate human rights and negatively impact society (to send before the election)
- Have we coordinated with international organizations like Access Now to send letters to the government to prevent a shutdown?
- Have we created and distributed resources for vulnerable communities such as at-risk human rights defenders, opposition groups, and marginalized groups to know what to do during a shutdown?

For during a shutdown:

- Have we prepared copy to post to social media and other channels about STOPPING an ongoing shutdown that we have circulated to coalition members and international partners?
- Do coalition members know who might need specific support during a shutdown?
- Do we have people in diverse areas of the country documenting the social and personal impact of shutdowns and prepared to report human rights abuses

For after a shutdown

- Do we have a plan to collect impact stories and documentation of human rights abuses that occurred during a shutdown?
- Do we have a plan to coordinate with journalists on accurate reporting of the shutdown and its impact?
- Do we have a plan to coordinate with lawyers on possible post-shutdown legal actions?

For more resources to help prepare for and advocate against shutdowns, visit www.preparepreventresist.org