Community Assessment on Internet Shutdowns in India

@SFLC Roundtable Workshop

Suggestions, Inputs & Recommendations by DEF & CSDD

July 2022

"Community Assessment on Internet Shutdowns in India"

@ SFLC workshop brief, 2022

Report by: Tuisha Sircar

CONTENT

I. Background

This report draws from the roundtable workshop for 'Community Assessment on Internet Shutdowns in India' which was organised by the Software Freedom Law Centre (SFLC) under Internews' OPTIMA project on the 8th July, 2022 in Delhi. The workshop participants ranged from Civil Society Organisations that engage in strategic litigation on key digital rights issues to research and implementing organisations engaged in digital rights advocacy and community outreach for digital inclusion in the grassroots. Digital Empowerment Foundation (DEF) - Council for Social and Digital Development (CSDD) participated in the focus group discussion on 'community support' in this context as a key stakeholder in the digital rights policy advocacy space and shared critical insights from DEF's various community engagement and intervention programmes across India.

The key agenda of the workshop was to discuss the key challenges, as well as potential solutions, to better prepare for and address Internet shutdowns in India based on a need assessment survey around internet shutdowns which was conducted by SFLC alongside the Bachchao Project. Based on the key findings of the survey, the participants engaged in proliferated discussions to find a way to address the issue of growing instances of arbitrary Internet Shutdowns in India.

II. Summary

This report highlights the key points from the discussion at the roundtable workshop for 'Community Assessment on Internet Shutdowns in India' which was organised by Software Freedom Law Centre in July 2022. The need for the workshop emerged from the increasing number of arbitrary internet shutdowns in India which has led to India being known as the the 'internet shutdown capital of the world'.

Highlights:

- "To safeguard national security" and maintaining law and order is cited as the primary reason for internet shutdowns. While protests and communal violence are 'legally' valid reasons for network shutdowns, there is no clearly defined reason for network shutdowns during exams other than 'cheating'.

- There is lack of transparency regarding the reason for shutdowns as well as lack of accountability through neglect of the due procedures as mentioned under the Temporary Suspension of Telecom Services Rules, 2017.

- Civil society is facing myriad issues regarding developing a robust advocacy strategy to challenge such arbitrary surveillance and control of the citizens despite their right to connectivity as being intertwined with other socio-economic and political rights as prescribed in the Constitution of India.

- Some of the specific challenges regarding advocacy against internet shutdowns in India are as follows: lack of mass collectivization due to less awareness and motivation amongst general masses; lack of wider strategic networking; lack of adequate resources, skills, tools and data; lack of strategic access to key stakeholders such as ISPs/Telecos etc.

- There is a need for urgent rethinking about the capacity that civil society as a collective requires to address the issues surrounding the multifarious processes of network shutdown in India as well as the deep social, economic, political and psychological impacts of it on people, businesses, emergency services and others.

Introduction

Internet shutdown can be broadly defined as the deliberate disruption of the Internet and relevant services. The aim is to control information received and sent by a group of people, by location or other characteristic.

Some of the other definitions are:

- *Access now (Hernandez, M. D., Anthonio, F. & Access Now Team. (2021). The Return of Digital Authoritarianism: Internet Shutdowns in 2021. Access Now: Keep It On) widely defines it as:*
  "An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called "blackouts" or "kill switches".

- *"An intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information".*

- *Digital Empowerment Foundation (Srivastava, R. (2017). Anatomy of Virtual Curfews: Human Rights vs National Security. DEF) defines it as:*
  "Virtual curfews or network disconnections/Internet shutdowns happen when telecommunications infrastructure, including mobile or Internet networks or both, are shut off or disrupted deliberately. During the time of network disconnection, phone calls or text messaging services or Internet-enabled services (such as WhatsApp, Facebook, etc.) are disrupted. The networks may be disrupted both technically and legally".
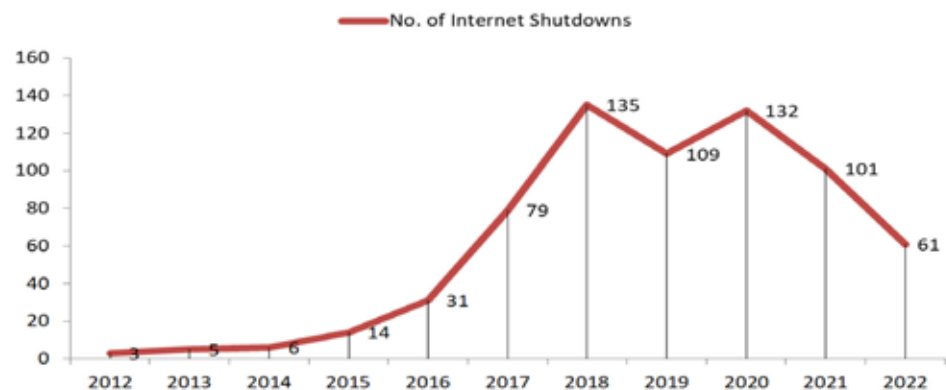
India has been deemed as the 'internet shutdown capital of the world' amidst increasingly growing instances of frequent and prolonged network shutdowns. In 2019 and 2020 alone, internet and allied services remained suspended in India for more than 13,000 hours, with Jammu and Kashmir witnessing the longest period of shutdown at 552 days.[1] In the wake of the abrogation of the erstwhile state's special status under article 370 by the centre, the internet, mobile and telephone connections were snapped in Jammu and Kashmir on August 4, 2019 and completely restored back on February 5, 2021.[2] While in 2021, the total hours of suspension of Internet and allied services in the country saw a dip from the previous year, till June 2022 the number of hours has increased multiple folds.

[1]Staff. (2021, December 4). India known as 'internet shutdown capital' of the world. The Federal. https://thefederal.com/news/india-known-as-internet-shutdown-capital-of-the-world/ (Last Accessed on: 10-7-2022)

[2]Express Web Desk. (2021, February 5). Restoration of internet services in Jammu and Kashmir: A timeline. The Indian Express. https://indianexpress.com/article/india/jk-4g-internet-mobile-timeline-7176408/ (Last Accessed on: 10-7-2022)

The government imposes shutdowns for various reasons, ranging from precautionary and preventive measures to curbing the spread of rumours during volatile situations. The most common reason given for such shutdowns is "to safeguard national security" and maintain law and order. However, the excuse of safeguarding national security as a justification for network shutdowns is used widely. With no definition of "national security" or threats to it spelled out in clear terms, citizens are never given precise reasons for shutdowns.

Internet Shutdowns in India (as on 19.7.2022)

— No. of Internet Shutdowns

[Line chart showing number of internet shutdowns by year:
2012: 3, 2013: 5, 2014: 6, 2015: 14, 2016: 31, 2017: 79, 2018: 135, 2019: 109, 2020: 132, 2021: 101, 2022: 61]

Source: SFLC Internet Shutdown in India Tracker[3] & The Anatomy of Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India Report by ICRIER.[4]

The United Nations in several instances has reiterated that access to the Internet is a human right and ensuring free access to the Internet is imperative to upholding human rights like the freedom of expression and freedom of assembly and association. Cutting off access to the Internet in this day and age, when a large portion of social and economic transactions take place online, not only takes away the right to free speech, expression, association and assembly but also infringes upon social and cultural rights. Journalists, activists, taxis and travel services, banking services, businesses, even emergency services like ambulances and medical are all adversely affected during shutdowns.

Moreover, not only do these government internet outages infringe on citizens' digital rights but they are also reckless acts of economic self-harm. According to Top 10 VPN, a leading Virtual Private Network review website, in 2019 the internet was shut down in India for 4,196 hours, and it cost the country more than $1.3 billion[5]; in 2020 the internet was shut down in India for 8,927 hours, and it cost the country more than $2.8 billion[6]; and in 2021 the internet was shut down in India for 1,157 hours, and it cost the country more than $5.83 million.[7]

---

[3]SFLC Internet Shutdown in India Tracker https://internetshutdowns.in/ (Last Accessed on: 10-7-2022)
[4]Kathuria, R., Kedia, M., Varma, G., Bagchi, K. & Sekhani, R. (2018). The Anatomy of Internet Blackout: Measuring the   Economic Impact of Internet Shutdowns in India. ICRIER.
[5]Woodhams, S. & Migliano, S. (2020). Government Internet Shutdowns Cost $8 Billion in 2019. Top 10 VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/2019/ (Last Accessed on: 10-7-2022)
[6]Woodhams, S. & Migliano, S. (2021). Government Internet Shutdowns Cost Over $4 Billion in 2020. Top 10 VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/2020/ (Last Accessed on: 10-7-2022)
[7]Woodhams, S. & Migliano, S. (2022). Government Internet Shutdowns Cost $5.5 Billion in 2021. Top 10 VPN. https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/ (Last Accessed on: 10-7-2022)

III. SFLC Workshop Highlights: Need Assessment Findings and Discussion

SFLC has been maintaining a real-time internet shutdown tracker for many years. However, the process of receiving real-time information on internet shutdown in India is complex and involves an inadequate process due to various reasons such as: self-reporting can be hindered with the network shutdown, self-reporting does not always work because affected citizens may not realise the shutdown has been imposed in the absence of an official notice, and media does not report on every shutdown.

a. Undefined and Unidentified: Problem in Recognizing Internet Shutdown

The assessment highlighted that there is a disjuncture between the actual number/length of the network shutdowns in the past and experience/memory of the respondents. People were not able to recall in detail the psychological, social and economic impacts of the shutdowns experienced by them in the past at any given moment. These outcomes could be due to the "hyper-local" nature of the shutdowns i.e., the regions or specific locations within a region. Moreover, there is a lack of standard understanding of what might be deemed as an internet shutdown since either all or specific aspects to internet access are affected which may lead to confusion, especially in the absence of official notice. It was also found that there are no visual cues on the device about the imposed network disconnectivity which confuses the users as sometimes some apps open and others don't or it could feel like endless loading/jamming.

b. Who is the Expert?

The respondents were asked about their expertise on internet shutdown in terms of its technicalities and legalities. The study found that people who have experienced internet shutdowns do not consider themselves as experts assumingly due to the points mentioned above, as compared to those who have never experienced internet shutdown.

c. Only Digitally Connected Respondents

The study mostly targeted urban areas which are usually digitally well connected and did not consider the gaps with those regions where internet is mostly inaccessible almost throughout the year or regions with complete inaccess to mobile network as well as internet.

d. The 'Why' in Internet Shutdowns in India

Most respondents reported having experienced internet shutdowns during volatile situations such as protests and communal violence. However, a significant number of respondents cited exams as the reasons for the same. While protests and communal violence are legally valid reasons for network shutdowns keeping in mind – Article 19 (2) (3) of the Indian Constitution, Section 69A(1) of the IT Act, 2000, Section 5 (1) (2) of the Indian Telegraph Act, 1885, and by the mandates of the Article 19 (3) of the International Covenant on Civil and Political Rights, 1966, Article 34 and 35 of the International Telecommunication Union Constitution – there is no clearly defined reason for exams other than 'cheating'. One of the reasons for such could be the public employment exams where 'cheating' can be considered as a political emergency. However, that still can be debated in a lot of ways since examinees usually find alternative ways of copying and exchanging answers beforehand in various ways such as through something called 'Bluetooth cheating'.

e. Bluetooth Mesh Networks as a Strategy to Circumvent Internet Shutdown

Circumventing the internet blockage using various Bluetooth enabled mesh networks has been in use. However, the knowledge and awareness of the same is lacking amongst most people. Moreover, in case of a wider area affected by the shutdown, mesh networks are not very useful.

f. Challenges for Strategic Litigation

Strategic litigation to challenge imposition of internet shutdowns is extremely dicey, largely because most shutdowns are short-term and the fact-checking and bureaucratic procedures involved arguing for a stay on a suspension order needs to occur within that short window. However, the recent case of Calcutta High Court staying a suspension order by the government of West Bengal directed towards prevention of 'cheating' in the class 10th exams[8] can be seen as a small victory.

g. Lack of Transparency and Accountability

Even in the aftermath of Anuradha Bhasin vs. Union of India, the suspension orders are often given on unconstitutional grounds which ignore the Temporary Suspension of Telecom Services Rules, 2017: 1) a large number of orders are issued by the District Magistrate instead of the Joint Secretary (or above) who has been duly authorised by the Union

---

[8]Bhaumik, A. (2022, March 10). 'Breaking: Calcutta High Court Stays WB Gov Order Temporarily Suspending Internet Services Amid Class 10 Board Exams [Read Order]'. Live Law.in. https://www.livelaw.in/news-updates/breaking-calcutta-high-court-stays-wb-gov-order-temporarily-suspending-internet-services-amid-class-10-board-exams-193850 (Last Accessed on: 18-8-2022)

Home Secretary or State Home Secretary; 2) many orders are still issued under the section 144 of the CrPC, 1973 without adequate reason or a situation of probable emergency; 3) there is severe lack of information about the proceedings of the review committee which is often not revealed even in RTIs. Such issues are not only a symptom of lack of transparency but also lack of accountability, especially in the absence of information that should be shared with the public regarding the rationale behind such orders.

h. High Economic Liability of the Users

The individual economic liability bore by the users/customers of the internet and other related services which are affected by network shutdown are extremely high: 1) The users/customers are not compensated for the loss of the services which they have paid for; 2) in case of a different subscription plan which can be utilised in case of mobile internet disconnectivity, the users/customers are charged an abysmally high amount which by far exceeds the standard amount charged under otherwise peaceful or normal circumstances.

i.   Stakeholder Outreach

Out of all the stakeholders, respondents cited ISPs/Telecos being the hardest to reach, followed by Government stakeholders, and Legislators. However, these stakeholders are also the most important to reach in order to fully understand the internal mechanisms of internet shutdown orders in India.

IV. Workshop Outcome: Need for Community Support and Advocacy Strategies

The phenomenon of internet shutdown in India is an amalgamation of various social, legal, political and technological processes that often has deep economic, social and psychological impacts. However, one major challenge that civil society faces is the lack of a mutually shared definition of shutdown of internet and other relevant services. Mutually agreed upon criterion to locate and understand instances of Internet shutdown and its multifariousness will allow the civil society to develop effective solutions against the arbitrary surveillance and control, as well as to create community resilience against economic, social and psychological impacts of it.

a. Mass Campaigning for Wider Reach

There is a growing normalisation of internet shutdown among the citizens due to which it is getting difficult to collectivise around the issue. Hence, engendering mass awareness on the issue has become critical. Unlike earlier campaigns for net neutrality which extended beyond the civil society space, the current issues on digital rights are not gaining enough traction among the general public. One reason for this could be the closing down of the civic space and disengagement of influential figures who have a good connect with the masses like social media influencers, comedians and other celebrities. One starting point could be bringing in these people into the fold for a wider reach of a collective campaign.

b. Need for a Wider Network amongst Civil Society Actors

There is a need for wider collaboration amongst the civil society actors which extends beyond the digital rights policy space. Digital rights needs to be viewed in tandem with other rights and a wider network that engages in human and civil rights issues needs to be created.

c. Capacity Building of the Communities

A multi-stakeholder approach needs to be adopted with the community stakeholders in the center whereby they are equipped with the relevant information, knowledge, tools and networks for realising their rights.

d. Localisation of Technology

There is a need for localisation of the technology so that it is accessible to people. In case of network disconnectivity or inaccess, web annotation could be relied on as a relevant model for information flow to the given communities. Moreover, creation of community access points which does not rely on direct GSM network in case of network disconnectivity or inaccess can also be fruitful. A significant focus should also be given on infrastructure reuse and resharing for sustainability of the technology, environment and finances.

e. Network Measurement as a Method to Study Internet Shutdown

Network measurement of internet shutdown in India using relevant softwares such as IODA, OONI and Clouflare Radar can be helpful tools for the civil society to study the specific technicalities such as volume of data and historical data of each internet shutdown.

f. Privacy and Safety tools during Internet Shutdown

Various digital tools and networks such as the Tella app, offline networks, VPN and mesh networks can be utilised for circumventing network shutdown and safeguarding confidential data in case of direct surveillance.

g. Documenting Lived Experiences of those affected

In order to understand the social, political, economic and psychological impacts of the internet shutdowns, lived experiences of the affected citizens needs to be documented with great detail with deep focus on the nuances. The understanding of the structural and direct violence experienced is of utmost importance.

h. Holding ISPs/Telecos accountable for user distress

By legally challenging the economic liability of the customers and the absence of compensation of the incurred loss, the civil society can create pressures on the ISPs/Telecos and hold them accountable. This provides a scope to legally challenge the practice of internet shutdown by the government in an indirect manner in the absence of any concrete alternative to the 'law and order' reason cited for the suspension orders.

Critical Points/Questions

- *1. There is a need to device an appropriate methodology to holistically study the mechanisms and impacts of the internet shutdown in India.*

- *2. Are the internet shutdowns imposed to curtail spread of misinformation or information? In case of the latter, what is the rationale?*

- *3. What are the long-term and short-term alternatives to Internet Shutdown based on the reasons cited for them? Should these alternatives also be based on technological solutions? Is circumventing the blockages using various digital tools a sustainable solution or is it just a quick fix?*

- *4. There is a need for detailed mapping of the issues, potential networks, needed resources, needed skills and alternative solutions.*

- *5. Is civil society equipped with the required capacities to deploy alternative strategies to combat shutdowns and censorships?*

V. DEF-CSDD Recommendations

Based on the findings of the need assessment and the discussions that ensued afterwards, Digital Empowerment Foundation (DEF) and the Council for Social and Digital Development (CSDD) are recommending the following points for not only building a strengthened community support mechanism but also to develop advocacy strategies against arbitrary internet shutdowns in India as well as its adverse multifarious impacts:

a.   **A multi-stakeholder approach** should be employed by the civil society to effectively gauge and address the community needs before, during and after instances of Internet Shutdown and other relevant services, especially in the states/UTs that are most affected like Jammu & Kashmir and Rajasthan. Consultation with the public in general could allow developing community strategies towards resilience and recovery against and from the impacts of Internet shutdown as well as render effective approaches to predict, prevent and respond to potential internet disruptions. Moreover, it is also important to engage the relevant public authorities and agencies to judiciously look at imposing internet shutdowns by being mindful of the fact that while such shutdowns are imposed to maintain law and order, it is simultaneously disrupting information-communication networks and leads to great economic losses.

b.   In order to **ensure continued access to emergency services** during the time of the shutdown or disruption, there is a need to collaborate with telecom operators. Moreover, access to communication with emergency services should be guaranteed to the public at all times, even during network shutdowns.

c.   There is a need for **creating a larger network of civil society actors** beyond the digital rights policy space. This network could strategize mass collectivization through campaigns advocating for connectivity as a fundamental right and engender awareness and support among the general masses for a digital rights movement in India.

d.   There is a need to **create a consumer grievance mechanism**. The government and telecom operators should come with solutions to report adverse impacts experienced during network shutdowns, including impacts on health, education and work. Government and companies should also explore how customers can be compensated for loss of access to services during network shutdowns.

e.   There should be **absolute transparency** regarding network disruptions in any given area. From informing the citizens about a network disruption to making the reviews of the review committee under the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 – available to the public.

f.   All **network disruptions should be logged/recorded**, and the government should publish an annual list of all shutdowns to maintain transparency and accountability within the system.

g.   To **reduce economic liability** of the users, financial losses incurred during network shutdowns should be adequately compensated by the government or telecom operators.

h.   There is a **need for robust researches** to not only understand the processes of network shutdown or disruption but also the impacts of it. A holistic research methodology would not just focus on mapping the economic, social and psychological cost of the shutdown but also focus on the variables between historical data and volume of data. Techno-ethnography, field-ethnography and discourse analysis of archival data could be used to theoretically and empirically map these processes across time and space.

i.   **Capacity building of the civil society actors** themselves is required for prompt and better responses in case of a network shutdown as well as to contain the negative effects imbued by such disruptions. One of the ways this can be done is by developing alternative technological solutions in the community such as by creating community access points. Imparting digital security training and creating solutions in case of direct surveillance must be kept in mind as well.

****

www.defindia.org