

# Commentary: Navigating Tensions and Stabilising Public Safety with Internet Shutdowns

Ivy Dhar\*

---

## 1. Introduction

Violence, ethnic clashes, and any form of social tensions that are likely to threaten public order may invite the imposition of temporary internet shutdowns as a precautionary measure by the Governments. The internet shutdown is an intentional disruption of internet-based communications in the region chosen for its implementation. Governments may resort to such measures on the basis that dissemination of fake news, rumour, and misinformation through internet access can fuel more violence.

Internet shutdowns in India are governed by the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, framed under the provision of Sec. 5(2) of the Internet Telegraph Act, 1885. Earlier, such shutdown orders were issued under Sec. 144 of the Code of Criminal Procedure, 1973 (CrPC). The Telecommunications Act 2023 adopted similar provisions regarding the temporary suspension of telecommunication services in the interest of public safety following a public emergency.

Human rights groups have opposed the internet shutdowns, calling them a digital ‘blackout’ (Human Rights Watch 2023). There are recurrent discussions on the range of collateral damages – including citizens incurring economic loss, and adverse impact on education and health care services – due to network disruptions, alongside issues of curbing people’s freedom to internet access. However, internet shutdowns remain a common practice during active conflict, protests, and events of political instability. And with the ascending frequency of social unrest, it is unlikely that the number of internet shutdowns will slow down.

As an example, the beginning of the year 2024 saw the protest called by the farmers’ collectives, which immediately led to the “suspension of mobile internet services, bulk Short Messaging Services (excluding banking and mobile recharge), and all dongle services provided on mobile networks except voice calls” in several districts of Haryana and Punjab (Jagga 2024).

Public inconvenience can be an outcome of the actions taken before reaching the normalisation of the emergency. Moreover, it is observed that the mechanism of control of the internet could be

---

\* Ivy Dhar is an Assistant Professor (Development Studies) at Dr. B. R. Ambedkar University Delhi.

intensely oppressive to segments of society who are socially and culturally vulnerable. Media reports have particularly highlighted the adverse effect of internet shutdowns during a conflict situation on women's safety, restricted mobility, and increased time lag in reporting violence against women (Chandran 2023). The question arises: while blocking information access and obstructing public connectivity, which is most essential to people who are already facing the consequences of the tensions, how will an assurance of public safety can be maintained?

This article emphasises that public safety alongside public emergency clauses used as a pre-requisite for internet suspension in India demands adequate attention, as it encompasses the core law and in the first place triggers the implementation of internet shutdowns—revisiting the term public safety is one of the major aims of this paper. Second, the paper tries to argue that despite the frequent use of shutdown measures there is a lack of clarity on the assurance of public safety by the Government. A recent Parliamentary Standing Committee report has discussed that Government in India has used internet shutdowns without assessing its impact on citizens and the economy and recommended a detailed study to assess its effectiveness in dealing with public safety and public emergency (Lok Sabha Secretariat 2023, 18) It further raised concerns that at present due to the lack of stipulated guidelines, the law enforcement agencies may resort to imposing telecom shutdowns on the basis of their own perceptions of disruptions in the law and order (Lok Sabha Secretariat 2023, 16). The discussion here does not aim to mark out a specific event, instead broadly examining the use of internet shutdowns as a policy measure during social unrest.

We start therefore by giving an overview of recorded numbers of shutdowns. The second section draws upon existing scholarly work to understand the digital public space. It argues for the protection of such space for an effective public safety outcome. To further guide the discussion and explore the applicability of public safety, we refer to the legal understanding and the observation report of a Parliamentary Standing Committee (2022-23) that was constituted for reviewing internet suspensions.

## **2. Growing Instances of Internet Suspensions: What's the Justification?**

There are no official estimates available for tracking the trend of internet shutdowns. Based on web-based research, it is found that India has witnessed around 690 instances of internet shutdowns between 2012- 2023 (SFLC 2024). It is observed that, since 2017, the incidence per year has been high around 70-130 shutdowns (Singh 2023). The most explicit type of internet shutdown is the absolute blackout of services, but there could be other types such as speed regulation or slowing down the internet. The target group at the receiving end was usually a group of areas, like tehsils (subdivisions), or districts, and in some instances the entire area of Indian states.

Internet shutdowns have been implemented in most of the Indian states, with some surging much ahead than others to block communication services on the pretext of an approaching threat. Jammu and Kashmir have faced repeated shutdowns, counting to more than 442 up to 2023 (Singh 2023).

The impact that the internet shutdown can cause is not indicated by measuring the instances or location alone, as a lot depends on the duration. Following ethnic clashes, Manipur experienced a prolonged period of internet shutdown spanning more than 200 days in 2023 (Chakraborty 2023). At times, a few days of lifting the shutdown may be sanctioned, or district-wise normalisation may be carried out, depending on the government's assessment of the situation. Globally, India has acquired a prime position to rush to suspend internet access for prevention against internal security threats and maintenance of order, notwithstanding that there may be other reasons too.

In response to UN Special Rapporteur David Kaye's public consultation on internet access, a study found that the most-commonly cited official justifications for internet shutdowns worldwide are national security, elections, protests and demonstrations, and also prevention of unfair means during examinations. In many instances, transparency surrounding processes that led to the implementation of internet shutdowns was absent, and the governments may have broadly justified causes as public safety or maintenance work (Access Now 2016).

Observing the pattern of internet shutdowns in India from 2012 onwards, it is seen that these were more for preventive action than reactive action. That is, they were mostly used as a precautionary measure to maintain law and order, and only in a few cases were shutdowns a step taken after a specific incidence of violence. In 2023, out of 95 internet shutdowns, 81 can be categorised as preventive ones, and only 14 as reactive (Basuroy 2024).

It is observed that the administrative orders may be a copy-paste of language, without specifying the incident that occasioned the preventive act of shutdowns. A study of around 26 internet shutdown orders, issued in a span of a year between 2020 and 2021 by the Rajasthan administration, reveals identical content in each order (Bapat 2021).<sup>x</sup> Though protests and political instability may be an immediate cause, however, these terms are rarely used in the justification language (Bapat 2021; Pankaj 2022).

The Supreme Court, in *Anuradha Bhasin v. Union of India* (AIR 2020 SC 1308), has laid out a requirement to maintain procedural safeguards on how internet and telecom shutdowns are to be imposed. The reforms remain far away in the regulatory frameworks, including the recent Telecommunications Act, 2023, which glosses over the existing shortcomings of the previous rules. The Act does not elaborate anything in the section on procedural safeguards, only uses a vague official explanation 'as may be prescribed', and therefore without specific prescribed norms the aim may get further diluted in the process of implementation.

### 3. The Digital Public Domain

The digital space, which is the information and online activity space, has become a significant category of public space. Low and Smith (2006, 5) have discussed that the definition of public spaces is very complex. It can be identified as ‘recognisable geographies of daily movement,’ and include the internet despite its ‘seeming[ly] spacelessness’. The digital space is no exception to other public spaces and demand appropriate public behaviour. Though digital spaces appear to be open and accessible to all people regardless of their social identity, its exclusionary nature cannot be ruled out.

Despite shortcomings, the number of active internet users stood at 759 million in India in 2021 and has been growing. Internet users engage in a range of activities, from online shopping (34%) and e-commerce (52%) to social media usage (70%), communications (77%) and entertainment (85%) (Kantar-IAMAI 2022).<sup>i</sup> This is evidence of an emerging active public life.

Scholars have also investigated whether the internet was evolving as a new ‘public sphere’. A functioning public sphere is understood as a communicative space that ‘can circulate information, ideas, and debates—ideally in an unfettered manner’ (Dahlgren 2005, 148). Kumar (2015, 136-137) argues for the potentiality of the internet, particularly social media, and confers it with a special role in a democracy by its capacity to develop a network between citizens, and between citizens and the political class. A ‘sense of public’ may be created and may eventually convert into votes. Though the internet has led to some interesting changes in the way democracy works, and internet freedom is conducive for ‘informed’ and ‘engaged’ public to evolve, but the design of unrestricted internet access might be a misleading aspect. Most national governments are using internet to defend their interests, and for dissemination of information; in turn, they decide the controls, and the limits of user rights.

Democratic states agree to the freedom of political and social expressions until they do not catch the flavour of revolution and are transacted within the framework of approved ideas. What fits the boundaries of public discourses in the internet space and establishing rules of ‘what is acceptable speech’ is not only difficult but ‘is inevitably political’ (Ricknell 2020, 111). Scholars argue that limiting the understanding of internet freedom is a serious reductionism that denies the public of its rightful share of opportunities (Kumar 2015, 135). The issue of internet access is not only about rights and freedom; it is a matter of usage and needs. Access to the internet has arrived at an age beyond technological convenience; it is more of a dependency and a necessity.

A large majority of internet users access the internet through mobile devices, and this proportion is expected to grow manifold in the coming years. The mobile device users (phones and dongles) stand at around 847.17 million, compared to wired subscribers which is around 36.87 million, and fixed wireless subscribers at 0.97 million (Telecom Regulatory Authority of India 2023). This aspect is important as the maximum shutdowns were targeted at mobile internet services, and only a few of them targeted both mobile and fixed-line internet services.

In the condition of shutdowns, the legitimised surveillance and information dissemination by the authorised platform companies gets curbed in the affected area. Studies discuss that without access to

the normal trusted sources of information, people may be willing to access any sources that are available, amplifying the scope of people moving to more unauthentic sources. This may leave people more exposed to harmful content, without the provision of fact-checking at the user's end (Shah 2021, 2695).

The regulatory shutdowns are often leaky and can be bypassed through human and technological backdoors. (ibid). Information is readily available on how to circumvent the local internet restrictions by connecting through Virtual Private Networks (VPNs). However, VPNs does not protect the users' privacy when browsing. (Elliot 2022). Misleading claims, distorted facts, or disinformation continue to remain active even after days of internet suspension, depriving the digital public space of authentic protection, with the possibility of a further dent in the mission of public safety.

Moreover, there are no significant studies globally that have objectively assessed how internet shutdowns have directly increased public safety, or if violence and security threats were curtailed by adopting shutdowns. Gohdes (2015, 367) has found that restricting information dissemination due to internet shutdowns have resulted in increased violence, as violent tactics are less reliant on effective communication in comparison to non-violent public dissent that relies on using the internet for organising grievances. Rydzak's (2019, 1) study on India also implies that the information vacuum during collective action as a result of shutdowns may compel participants to substitute non-violent tactics with violent ones. A critical mission of the temporary internet shutdown – to stop spreading propaganda – does not seem to have achieved much.

#### **4. Balancing the Motive of Public Safety with Ground Reality**

Public emergency remained a vague expression even after its use for decades, carried down from the colonial era. The terms 'public emergency' and 'public safety', not defined in the statute of the telecom suspension rules, tend to be stretched with concerns where these aspects may not be applicable. The Parliamentary Standing Committee admitted in its report that since public emergency and public safety are the only grounds for imposing internet shutdowns, and without a clear-cut definition, the gravity of its use by the State governments remains open-ended for misinterpretation. It came to be used in a purely subjective manner, relying on the ground situation assessed by the district officers (Lok Sabha Secretariat 2023, 46).

What might be an issue of local crime and routine policing were often given the nature of emergency and safety threats. The authorities have almost a free hand to determine the usefulness and applicability of shutdowns, and what they perceive as detrimental to public safety. There is a consistent emphasis on the issue of transparency and clarity, given that internet shutdowns are being used as an instant means for maintaining order. The need of the hour is to define the parameters of public emergency and public safety to rule out ambiguity in the decisions and actions of the State governments (Lok Sabha Secretariat 2023, 46).

The Supreme Court in *Hukam Chand Shyam Lal v. Union of India and Others* (AIR 1976 SC 789) has specified that any other kind of emergency is not to be confused with a public emergency. Further, in *People's Union of Civil Liberties v. Union of India* (AIR 1997 SC 568), the Court distinctly mentioned that a public emergency must be declared only when there is a prevailing condition affecting the people at large, subject to overcoming it with an immediate action.

*Anuradha Bhasin v. Union of India* (AIR 2020 SC 1308) was a landmark judgment on the question of internet suspension. It revisited the *Hukum Chand Shyam Lal* case to observe that public emergency is to be determined as 'sudden and its consequences are grave', primarily subject to the interest of public safety, and concerns the security of the State.

In much earlier pronouncements, the Supreme Court in *Brij Bhushan and another v. The State of Delhi* (1950 SC 605) established that public safety acquired a well-recognised meaning juxtaposed with the maintenance of public order. To observe a deeper sense of the term, the court distinguished it with public 'unsafety', which is to be usually 'connected with serious internal disorders and such disturbances of public tranquillity' that 'jeopardise the security of the State'.

In *Rajeev Kumar @ Monu Shukla v. State Of U.P* (Writ - C No. - 31473 of 2019), the Court clarified with the support of previous pronouncements that public safety does not mean any ordinary disturbance of law and order, rather it means the safety of the public at large.

The courts have broadly interpreted public safety as something that affects the community at large and is indispensable to the larger social interest. Maintaining public safety is a legitimate state concern. However, actions towards its implementation must carry safeguards that protect the interest of both the state and the public, whom the state seeks to protect. By the precedent of the Court cases, one may say the terms public emergency and public safety must not be used as a blanket mechanism. Any authority determining if any situation involves a threat to the public order must carry accountability for a responsible decision. The Supreme Court's guidelines allow discretion to governments with certain limitations.

It can be inferred that public safety is not as ambiguous as the legislative rule treats it to be. The use of the term must be seen in a 'means and ends' spectrum. Following legal and Committee report discussion that warned against the subjective notion of public safety authority must make assessment of the presence or apprehension of 'danger' to public safety. Indicators can be devised by examining the First Information Reports (FIRs) showing serious damage to public utilities and threats to public peace (Chatterjee 2020, 9). In the aftermath of imposing the shutdown, to prevent any further danger to public safety, caution must involve ensuring the utility services and government assistance are within reach to people, primarily if it is a conflict-ridden situation.

'Public safety' is seen for more than a hundred years of law as government protection of persons or property from sudden and violent injury, but it often gets narrowly defined as physiological protection. With the expansion of the protection aspect to include well-being as per the development goals, any threat to basic needs and opportunity worthy of protection must encompass public safety (Friedman 2021, 13-19).

In an attempt to reimagine public safety applicable to the scope of growing public needs, experts have discussed the practical necessity of online network platforms between community and law enforcement agencies, among other measures, to enable effective public safety (Prabhakar, Gupta, and Mehrotra 2015). It can be argued that the public safety clause needs more strengthening, which otherwise weakens due to an emergent situation of tension and unavailability of information services due to the shutdowns.

The shutdown debate is often weighed by considerations of freedom versus safety. Both aim at keeping the public at the central point, so either way, neither should be easily compromised. Owing to the limited capacity of government monitoring mechanisms, internet shutdowns may amplify threats to safety, due to heightened vulnerability during a public emergency. It is widely discussed that internet shutdowns seriously hamper real-time reporting and obstruct the coordination of agencies and the public. For example, unless the public is prepared in advance for the emergency, the people may find difficulty to seek government helplines, given the reliance placed on the internet for information scouting.

Experts have suggested democratic gatekeeping is a viable option, where platform companies strictly filter or delete undesired information in the areas affected. The most agreed consensus from all quarters is that internet shutdown measures must be used as the last resort rather than the first for public safety intentions, and only after a thorough assessment of conditions inciting public emergency at the conflict-hit sites.

## References

- Access Now. 2016. "Primer on internet shutdowns and the law." Last modified November, 2016. Retrieved February 20, 2024 from [www.accessnow.org](http://www.accessnow.org).
- Bapat, Krishnesh. 2021. "[Revealed] Udaipur Internet Shutdown Orders: Cut, Copy, Paste!." Internet Freedom Foundation. Last modified November 1, 2021. Retrieved March 30, 2024 from [www.internetfreedom.in](http://www.internetfreedom.in).
- Basuroy, Tanushree. 2024. "Number of internet shutdowns in India from 2012 to 2024, by type." Statista. Last modified February 22, 2024. Retrieved March 30, 2024 from [www.statista.com](http://www.statista.com).
- Chakraborty, Debducta. 2023. "India shut internet more times than any other country in 2023. Manipur blackout Northeast's longest." *The Print*. December 31, 2023. <https://theprint.in/india/india-shut-internet-more-times-than-any-other-country-in-2023-manipur-blackout-northeast-s-longest/1906283/>
- Chandran, Rina. 2023. "India's Internet Shutdowns Hurt Women More, Manipur Assaults Show." *The Wire*. July 28, 2023. <https://thewire.in/security/indias-internet-shutdowns-hurt-women-more-manipur-assaults-show>.

- Chatterjee, Siddhant. 2019. "Exploring Possible Solutions to Curb Internet Shutdowns in India." The SSRN, Last modified November 7, 2019. Retrieved February 25, 2024 from <http://dx.doi.org/10.2139/ssrn.3644879>.
- Dahlgren, Peter. 2005. "The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation." *Political Communication* 22 (2): 147–162. <https://doi.org/10.1080/10584600590933160>.
- Elliot, Vittoria. 2022. "Five Ways to Stay Online During a Government Internet Shutdown." *Global Investigative Journalism Network*, May 11, 2022. <https://gijn.org/stories/five-ways-to-stay-online-during-a-government-internet-shutdown-gijn/>.
- Friedman, Barry. 2021. "What is Public Safety?" Public Law Research Paper No. 21-14, NYU School of Law. Last modified September 19, 2022. Retrieved February 25, 2024 from <https://ssrn.com/abstract=3808187>.
- Gohdes, Anita R. 2015. "Pulling the Plug: Network Disruptions and Violence in Civil Conflict." *Journal of Peace Research* 52 (3): 352–367.
- Human Rights Watch. 2023. "No Internet Means No Work, No Pay, No Food." Last modified June 14, 2023. Retrieved March 30, 2024 from [www.hrw.org](http://www.hrw.org).
- Jagga, Rakhi. 2024. "Internet ban in Punjab, Haryana deals a blow to students taking exams, other vital services." *The Indian Express*, February 21, 2024. <https://indianexpress.com/article/cities/chandigarh/farmers-protest-mobile-internet-ban-punjab-haryana-9172316/>
- Jayant, Pankaj. 2022. "Mapping the Rising Internet Shutdowns in India since 2016." *The Wire*. October 09, 2022. <https://thewire.in/government/mapping-the-rising-internet-shutdowns-in-india-since-2016>.
- Kantar-Internet and Mobile Association of India (IAMAI). 2022. "Internet in India 2022." Last modified April, 2023. Retrieved February 27, 2024 from [www.iamai.in](http://www.iamai.in).
- Kumar, Nishant. 2015. "Internet Freedom, Social Media, and Internet Democracy: Prospects and Challenges." *The Indian Journal of Political Science* 76(1): 135–146.
- Lok Sabha Secretariat. 2023. "Standing Committee on Communications and Information Technology: 37<sup>th</sup> Report." Retrieved February 20, 2024 from <https://loksabhadocs.nic.in>.
- Low, Setha and Smith, Neil. 2006. *The Politics of Public Space*. New York: Routledge.
- Prabhakar, Vishvesh, Gupta Sanjeev and Mehrotra, Rajul. 2015. "How to transform public safety in India." *The Economic Times*, July 27, 2015. <https://economictimes.indiatimes.com/news/politics-and-nation/how-to-transform-public-safety-in-india/articleshow>.



- Ricknell, Emma. 2020. "Freedom of Expression and Alternatives for Internet Governance: Prospects and Pitfalls." *Media and Communications* 8 (4): 110–120.
- Rydzak, Jan. 2019. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." The SSRN, Last modified February 7, 2019. Retrieved March 31, 2024 from SSRN: <https://ssrn.com/abstract=3330413>
- Shah, Nishant. 2021. "(Dis)information Blackouts: Politics and Practices of Internet Shutdowns." *International Journal of Communication* 15: 2693–2709.
- Software Freedom Law Centre India (Slfc.in). 2024. "*Government of India extends Internet Shutdown in Punjab.*" Last modified February 27, 2024. Retrieved March 31, 2024 from [www.https://internetshutdowns.in](http://www.https://internetshutdowns.in).
- Software Freedom Law Centre India (Slfc.in). 2024. "*India's Shutdown Numbers.*" Retrieved April 09, 2024 from [www.https://internetshutdowns.in](http://www.https://internetshutdowns.in).
- Singh, Subham. 2023. "Manipur: Violence-hit State Tops Internet Shutdowns in India in 2023 with 83 days of Blackout." *India Today*, July 25, 2023. <https://www.indiatoday.in/diu/story/manipur-violence-hit-state-tops-internet-shutdowns-india-blackout>.
- Telecom Regulatory Authority of India (TRAI). 2023. "*Press Release No.66.*" Last modified December, 2023. Retrieved March 31, 2024 from [www.traigov.in](http://www.traigov.in)

## Notes

---

<sup>i</sup> The data recorded is for a year on all segments. Online shopping refers to shopping through Amazon, Flipkart, etc. E-commerce is measured by access to online shopping, online finance, online travel, etc. Social media refers to those who have accessed content on social media websites or platforms. Communication means those who have done text/ voice/ video chat or used email, video conferencing, etc. using an online website or app. Entertainment covers those who are either Online Video Viewer, or Online Music Listener, or Online Gamer (Kantar-IAMAI 2022).