



Internet Censorship and it's challenges in India: - A Socio-Legal study

¹Anuj Kumar Singh (Research Scholar)*

²Dr. Nidhi Sharma (Associate Professor of Law)
 Faculty of Law, Agra College, Agra

Abstract

For every free individual to govern themselves, they must be open and free to express themselves- openly, repeatedly and publicly; whether in writing and speech or through online platforms. The right to free speech is a fundamental concept of every democratic country, where the people of that country have full right to choose or remove their elected representative as per the workings towards the nation for which he/she was elected. For the wrongdoings of the authoritative figures of a country, free speech holds up the pragmatic idea of criticizing various schemes or policies passed and regulated in the very country. However, in India internet censorship creates a big obstacle in balancing this right with public safety in our digital age. Article 19 (1) (a) of the Constitution of India protects free speech and expression. On the other hand Article 19(2) gives wide powers to the government in limiting this speech for safety, order and morals of the country. Section 69A of the Information Technology Act of 2000, lets the government to block posts or websites in order to stop hate speech, fake news and violence in our diverse society without the intervention of courts. The 2021 IT Rules endanger personal privacy and stifle free expression by forcing apps to track who sent a message. What began as a safety measure has now evolved into a tool for state power, effectively depriving the internet of its core identity as a sphere for free expression. Our findings illustrate the depth of how the misuse of digital censorship in India is posing a grave threat to both personal privacy and the future of a free internet.

Keywords: Freedom of Speech, Internet Censorship in India, Section 69A of the IT Act, 2000, Digital Privacy, IT Rules 2021

Received: 08/01/2026

Accepted: 26/02/2026

Published: 28/02/2026

*Corresponding Author:

Anuj Kumar Singh

Email: ankus0102@gmail.com

INTRODUCTION

Imagine a college student from a small city shares a post on a social media handle criticizing a newly introduced government policy. The

shared post does not contain any threats, warnings or derogatory speeches against the government; however, it simply questions the impact of the decision on society. A few hours later the post is deleted, and the student receives a notice stating that the content violated or

infringed upon guidelines related to public order. Furthermore, no detailed explanation is given. Followers of the student begin deleting their own posts out of fear, and the student hesitates to speak online again, worried about possible legal trouble or social backlash.

This example portrays how censorship can create a sense of uncertainty and fear, even when the intention was harmless.

In the same manner, Internet Censorship in India has become a serious socio-legal issue in this contemporary digital era. As internet access expands across different cities and villages, questions arise regarding how far the State can regulate online content without harming democratic values.

HISTORICAL CONTEXT OF CENSORSHIP LAWS IN INDIA:

- **Roots in Colonial Era: -**

During the British Colonial period in India, the internet censorship laws were introduced as in the form of strict media by the rulers in order to silent dissent. The Vernacular Press Act of 1878 targeted the local newspapers for criticizing the policies made by the governing body. The Indian Telegraph Act of 1885 grants the state legal authority to monitor communication and suspend digital networks. These set a pattern of state authority over information.

- **Post- Independence Framework: -**

After India got its independence in 1947, the Constitution under clauses of Article 19 provided freedom of speech and expression but with reasonable restrictions in order to safeguard the integrity of the country and public order at the same time. In the initial phases laws like the Press and Registration of Books Act (1867, adapted) continued controls. The National Emergency (1975-1977) imposed under Indira Gandhi saw heavy press censorship, which set an example of how leaders can use laws to hold power and suppress dissent to retain political control.

- **Rise of Digital Laws: -**

When internet arrived in India in 1995, new rules were introduced. To regulate e-commerce and cybercrimes, IT Act was passed in June 2000. This landmark act criminalized obscene online content and gave search powers to police without any warrants.

- **Key Amendments and Blocks: -**

A major 2008 IT Act amendment enhanced censorship through Section 69A, enabling the blocking of sites for public order or sovereignty without court intervention. In 2015, over 850 porn sites were blocked under Section 79(3)(b) after a court petition.

- **Shutdowns and Recent Shifts: -**

Since 2012, India leads global internet shutdowns, citing the Telegraph Act, 1885. IT Rules 2021 mandated the online platforms to trace messages and remove posted content swiftly which gave rise to privacy concerned debates in the country. The 2024 sahyog platform boosted local censorship powers, yet precedents like Shreya Singhal and Anuradha Bhasin mandate strict legal clarity and proportionality against such expansions.

LEGAL FRAMEWORK: IT ACT AND SECTION 69A: -

- **Overview of IT Act, 2000: -**

The Information Technology Act, 2000 was passed on October 17, 2000 for tackling cyber related issues, supporting online businesses and fighting computer crimes. This Act gave protection to the user's data and delivered legal status to e-records. Cyber activities like hacking, fake emails, and harmful online contents are punishable under the code.

- **Introduction of Section 69A: -**

In 2008, IT Act was amended and Section 69A was added. This amendment brought significant changes where the central government was given strong powers to block public access to online information. This clause authorizes the government to order any agency or any internet company to restrict certain content online to

protect and safeguard India's sovereignty, integrity and defense.

- **How Section 69A Works?**

According to Section 69A, anyone- like police, a government office or even citizens can report about the harmful content. The details regarding the content gets delivered to a "nodal officer", who further passes it to a "designated officer" in the IT Ministry. This designated officer forms up a committee of experts from the fields of IT, Law and Security to study the complaint and discuss whether blocking the complained content makes sense or not. Furthermore, the committee's advice is sent to the Secretary of the Ministry of Electronics and Information Technology (MeitY) for the final decision.

CASE STUDY: - Shreya Singhal v. Union of India – A Landmark for Free Speech

- **Background of the Case: -**

The case emerged as a growing concern over the misuse of Section 66A of the IT Act, 2000. Across the different regions of India, many individuals were arrested for the posted comments on the social media handles. A significant incident took place in 2012, when two young women were brought under custody over a Facebook post that inquired about the shutdown of Mumbai following the demise of a political leader. Their arrest sparked nationwide anger and debates regarding freedom of

expression online. Many highlighted and claimed that the law was vague and easily misused. Shreya Singhal, a law student approached the apex court and challenged the validity of Section 66A.

- **What was Section 66A?**

Section 66A of the IT Act interpreted that sending messages online that are “grossly offensive”, “menacing” or “causing annoyance or inconvenience” will be considered a criminal offence. Many claimed that this section was being misused to silence criticism as the law gave wide powers to the police to arrest people for online speech.

- **Main Legal Issue: -**

Section 66A of the IT Act raised a serious question before the apex court: whether the section violated the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution. However, this democratic right is not absolute. Article 19(2) elucidates that such a fundamental right is subject to reasonable restrictions, but only on the clear grounds of public order, defamation, incitement to an offence, sovereignty and integrity of India, security of the State, and friendly relations with foreign countries.

The main issue with Section 66A of the IT Act was its interpretation that sending messages

online which are “grossly offensive”, “menacing” or “causing annoyance or inconvenience” would be considered a criminal offence. These expressions were unrelated to any of the specific grounds of Article 19(2). The petitioners argued that this section was overly broad, vague and capable of being misused against any naïve individual, including those criticizing the government.

Therefore, the Court had to examine whether the section fell within constitutional limits or exceeded them by unduly restricting free speech and expression.

- **Supreme Court’s Reasoning: -**

The apex court highlighted two points. First, it stated that Section 66A was uncertain and vague; second, terms like “offensive” and “annoying” are subjective and vary per person.

The judges also explained the important distinction between discussion, advocacy and incitement.

- **Final Judgment: -**

The Supreme Court in 2015 struck down Section 66A of the IT Act completely and held it unconstitutional.

The Court upheld Section 69A, which permits website blocking, and clarified intermediary liability under Section 79. It ruled that platforms

are not automatically responsible for content unless they receive a formal legal notice.

- **Importance of the Judgment: -**

This landmark ruling secured Indian digital free speech by shielding citizens from arbitrary arrests over online posts. It invalidated vague laws used to silence critics, reinforcing democracy. Now, people can share opinions freely, knowing that only speech causing direct, immediate harm can be legally restricted.

REGULATION OF OTT PLATFORMS

Under the Information Technology (IT) Rules, 2021, the largely unregulated Over the Top (OTT) platform market in India has given way to a structured three-tier framework. Although recent government actions show a significant tightening of accountability, OTT content is not subject to pre-censorship by the Central Board of Film Certification (CBFC), unlike theatrical releases.

- **Present Regulatory Structure (IT Regulations, 2021)**

Through the Ministry of Information and Broadcasting (MIB), the government uses a "soft-touch" regulatory approach to manage OTT platforms.

- Level I: Publishers' Self-Regulation**

Platforms are required to set up an internal grievance procedure. Complaints must be acknowledged by a designated Grievance Officer within 24 hours and resolved within 15 days.

- Level II: Industry Bodies' Self-Regulation**

Publishers are required to become members of a self-regulatory organization led by a retired judge from the Supreme Court or High Court. These organizations, like the Digital Publisher Content Grievances Council (DPCGC), handle unresolved complaints and make sure the Code of Ethics is followed.

- Level III: Supervision by the Government**

The final oversight mechanism is an Inter-Departmental Committee that the MIB established. Section 69A of the IT Act allows the government to issue emergency take-down orders for content that poses a threat to public order or national security.

- **Important Requirements for Compliance**

Age-Based Classification: U (Universal), U/A 7+, U/A 13+, U/A 16+, and A (Adult) are the categories into which content must be divided.

Access Controls: Platforms must use trustworthy age verification for "A" rated content and parental locks for content rated U/A 13+ or higher.

Timelines for Content Takedown: Sensitive content (nudity, impersonation, or privacy violations) must be removed within 24 hours of a valid order, while unlawful content must be removed within 72 hours.

- Current Trends and Developments (2025–2026)

Strict Enforcement and Bans: In 2025, the government banned 25 over-the-top (OTT) platforms and another 18 platforms for distributing "obscene and sexually explicit content" passing as web series as part of a massive crackdown.

Proposed "Digital Code 2026": According to reports, the government is creating new regulations to define "obscene" content more precisely and impose a mandatory age classification system akin to that of movie certification.

The "Censorship" Debate: Critics contend that the three-tier system and recent advisories (following controversies like India's Got Latent) cause creators to self-censor out of fear of legal action, despite the government's insistence that content is outside the CBFC's jurisdiction.

Judicial Position: To safeguard public morality and religious sentiments, the Supreme Court and several High Courts have called on the government to strike a balance between "reasonable restrictions" and creative freedom.

CENSORSHIP OF DIGITAL NEWS MEDIA

Internet censorship is the intentional suppression or restriction of online content by governments and private organizations, with a focus on digital news media. This has changed in recent years from intermittent blocking to formalized regulatory frameworks that detractors claim stifle democratic accountability and independent journalism.

- India's Present News Media Censorship Situation

By February 2026, new regulations and enforcement measures had significantly tightened the digital news environment in India:

Three-Hour Takedown Window: New regulations, which go into effect on February 20, 2026, require social media companies (Meta, YouTube, X) to take down "unlawful" content within three hours of being notified. This is a significant cutback from the previous 36-hour deadline.

In order to categorize online content producers as "digital news broadcasters," the proposed Broadcasting Services Bill would require them to set up self-funded Content Evaluation Committees (CEC) in order to pre-approve content and post it.

Mass Withholding of Accounts: The government directed X to block more than 8,000 accounts in May 2025, including those of prominent news

organizations such as The Kashmiriyat, Maktoob Media, and The Wire.

Institutional Erasure: According to reports, there is a "digital vanishing act" taking place in which important investigative pieces about surveillance and human rights are being removed from online archives due to legal pressure.

- Legal Censorship Mechanisms

The Information Technology (IT) Act, 2000 is the main tool used by the Indian government to control digital content:

In the interest of public order, sovereignty, or national security, Section 69A gives the authority to block content. Many orders are still confidential, which limits the affected media's legal options even though the Supreme Court (in *Shreya Singhal v. Union of India*) required that the reasons for such orders be documented in writing.

A grievance redressal system with three tiers was established by the IT Rules, 2021. Government bureaucrats can summarily order the deletion of digital news articles in the last tier.

Takedown notices are sent to "intermediaries" (platforms) under Section 79, which threatens to revoke their legal immunity if they don't comply.

- Technical Suppression Techniques

To limit access to digital news, censors use a number of technical tactics:

- IP and DNS blocking involves rerouting domain name requests to "Not Found" pages or preventing users from accessing particular server addresses.
- Keyword filtering is the process of automatically looking for sensitive terms in URLs or page content to initiate instantaneous blocks.
- Algorithmic suppression and shadow banning: reducing the visibility of specific account or hashtags without completely blocking them.
- Internet shutdowns: Total cessation of services in particular areas, like the recent blackouts in Manipur and the 552-day shutdown in Jammu and Kashmir (2019–2021).

- Global Background and Significance

Press Freedom Rankings: As of July 2025, India's standing on the Reporters Without Borders (RSF) index had progressively deteriorated, falling to 151 out of 180 nations.

The "Arms Race" is the ongoing rivalry between censors and those who create tools for circumvention. To access censored news, millions of users around the world rely on decentralized hosting (like Zero Net), VPNs, and the Tor browser.

Economic Cost: Between 2012 and 2017, India's internet outages were estimated to have cost the country's economy more than \$3 billion.

COMBATING MISINFORMATION AND DEEPPAKES

In February 2026, pre-publication control and rapid-response mandates replaced reactive moderation as the approach to countering false information and deepfakes.

- Framework for Accelerated Takedown (India 2026)

India's revised IT regulations, which go into effect on February 20, 2026, set the strictest removal deadlines for digital platforms in the world:

- **3-Hour Window:** Content that has been declared "unlawful" by a court or government order must be taken down by platforms (Meta, X, YouTube, etc.) within three hours.
- **2-Hour Window:** The deadline is shortened to two hours for "highly sensitive" content, which includes intimate imagery and non-consensual deepfake nudity.
- **Conditional Safe Harbour:** If intermediaries don't label AI content or don't meet these windows, they could lose their Section 79 immunity and be held legally responsible for user posts.

Required Labeling and Provenance

New regulations demand that synthetic media be clearly distinguished in order to lessen the "cognitive load" on users:

- **Prominent Labels:** Any audio, video, or image produced by AI must have a watermark labeled "Synthetically Generated" or a spoken disclaimer.
- **Permanent Metadata:** In order for investigators to identify the precise AI tool and creator, platforms must incorporate machine-readable metadata, also known as digital fingerprints, into files.
- **User Disclosure:** During the upload process, users are now legally obligated to disclose whether their content is artificial intelligence (AI) generated.

-Advanced Technologies for Detection

By 2026, detection methods have advanced to include biological and cryptographic signals in addition to pixel analysis:

- **Biological Signal Detection:** Programs such as Intel's Fake Catcher analyze subtle facial blood flow patterns (photoplethysmography) that AI finds difficult to mimic.
- **Cryptographic Verification:** Amber Authenticate creates a tamper-proof trail from

camera to screen, demonstrating authenticity at the time of capture.

- **AI-Powered Monitoring:** To identify deepfake campaigns before they become widely known, platforms such as Cloud SEK offer real-time monitoring across social media and the dark web.

- International Regulatory Strategies

The Jurisdiction Strategy's Principal Mechanism

European Union Risk-Based the EU AI Act (2024) requires generative AI to be transparent, with the majority of its provisions going into effect in 2026.

China Preemptive mandates mandatory labeling and real identity verification for AI users starting in 2023.

The US sector depends on a patchwork of federal anti-fraud oversight and state laws (such as California's AB 972 for pornographic deepfakes)

The Online Safety Act gives Ofcom the authority to penalize platforms that fail to reduce the risks of deepfakes under the UK Duty of Care.

- Risks and Difficulties

The move to "pre-publication control" in 2026 has generated a lot of discussion:

Over-censorship: In order to avoid liability, experts caution that the 3-hour window may

compel platforms to employ "automated hammers" that inadvertently eliminate satire, parody, and reliable news.

Resource Inequality: Smaller platforms might not be able to afford 180-minute compliance, but Big Tech can afford round-the-clock legal and detection teams.

The AI "Arms Race": Deepfake generators become increasingly evasive as detection tools advance, frequently surpassing the legislative cycle.

THE CHILLING EFFECT ON EXPRESSION

In February 2026, new regulations that compel platforms and individuals to put risk avoidance ahead of free speech have increased the "chilling effect" on digital expression.

- February 2026: The Regulatory Trigger

As of February 20, 2026, India's revised IT Rules have added a number of high-pressure measures that support a self-censorship culture:

Platforms are required to take down "unlawful" content within three hours of receiving a notice from the government or a court. Because there is no longer any time for human legal review, platforms are being forced to remove excessive amounts of content automatically in order to preserve their "safe harbour" immunity.

Vague Definitions: The regulations target "false" or "misleading" "synthetically generated information" (SGI) without giving clear definitions. Because of this ambiguity, users avoid sharing anything, even parodies or satire, for fear of being flagged.

Legally, users must now self-declare any content created by artificial intelligence (AI) before publishing it. Under the Bharatiya Nyaya Sanhita (BNS), failure to do so may result in account bans or other legal repercussions, which would discourage innovative or creative digital work.

- Influence on Public Conversation and Journalism

The landscape of 2026 demonstrates a clear change in the dissemination of political and news viewpoints:

Journalistic Self-Censorship: According to international reports from late 2025 and early 2026, journalists' self-censorship has increased by 63%. Because of the risk of instant digital erasure and legal retaliation, reporters in India—particularly those in rural areas—are increasingly avoiding "difficult questions" about corruption or sand mafias.

The "Regulated Gallery" Effect: Instead of serving as a "Town Square" for discussion, social media is evolving into a "Regulated Gallery" where only narratives that have been approved by the state can freely circulate.

Privacy-Induced Chilling: People change their speech and thoughts because they believe they are "being watched" due to perceived surveillance, such as the requirement that platforms include permanent metadata identifiers in content.

- Social and Psychological Aspects

The chilling effect has evolved into internalized obedience rather than just the fear of going to jail:

Social Conformity: Because algorithmic "echo chambers" reinforce the opinions of the majority, dissenters feel alone and are less inclined to voice their opinions because they perceive a lack of social support.

Risk Aversion: According to research from 2025–2026, people who are risk averse are 28% more likely to stop participating in digital discourse altogether when regulations are unclear, thereby stifling moderate and non-political voices.

Asymmetric Expression: Conservative or moderate opinions report higher levels of self-censorship to protect their reputations, while progressive or liberal voices frequently stay outspoken on sites like X.

INTERNET SHUTDOWNS: PATTERNS AND PROPORTIONALITY TEST

Internet shutdowns are commonplace in India, ostensibly to preserve public order. In the course of issuing internet shutdown orders pursuant to the Suspension Rules of 2017 a number of states around the Nation have cited threats to National Security (terrorism, public disorder) as the source of their authorization of such orders. But now the socio-economic impact of internet shutdowns is well established on education and health services. In the legal sense the primary measure is the "Proportionality Test," (i.e., the government must demonstrate that the internet shutdown was the least restrictive means available). Courts also now require that all orders for internet shutdowns are to be made public and periodically reviewed. However, due to the frequent application of Section 144 of the Code of Criminal Procedure (CrPC) (a competent authority to suspend the provision of internet), there are no required procedural safeguards during the exercise of this power (improper actions will be held unlawful). It has become clear that the continued use of Executive authority in issuing internet shutdown orders is becoming standard where "Emergency" justifications continue to be put forward rather than only formally invoked as the last resort. In examining how the courts have sought to address the overreach of the Executive when issuing orders for internet shutdowns, the courts are now requiring the use of transparent and scientific criteria in all internet shutdown orders. The difficulty in addressing internet shutdowns lies in preventing the misuse of this authority for the

mere convenience of the Administration. The objective of the courts remains to ensure that the power of the state to disconnect citizens will continue to only exist when constitutionally justified.

ANURADHA BHASIN V. UNION OF INDIA : ACCESS AS A RIGHT

The Anuradha Bhasin verdict in 2020 is an important milestone for digital rights after the blackout in Jammu & Kashmir. The Supreme Court decided that freedom of expression and right to conduct business over the internet are both protected by Article 19 of the Constitution. The court did not adjudicate whether access to the Internet is a stand-alone fundamental right. However, it did rule that it is a necessary means for exercising these other rights. Therefore, any limitation imposed on access to the Internet has to comply with the "Reasonable Restrictions" clause of Article 19(2). The court also ruled that suspension orders must be published and are subject to judicial review and ruled, effectively, that indefinite shutdowns are illegal. As per the judgment, suspension of Internet services is a very drastic measure only to be used in cases involving immediate threats to public safety. This ruling also forced the Government of India to reassess its use of total internet blackouts and accept that digital access is an integral part of modern democratic participation and cannot be summarily denied under the guise of protecting national security.

JUDICIAL OVERSIGHT VS. EXECUTIVE POWER

The Indian system of censorship can be described as a balance between judicial review and executive authority. The executive has very wide-ranging powers under Section 69A of the IT Act in relation to restricting access to information for reasons that include national integrity and order. It does so through opaque processes, meaning that there is little opportunity for external accountability or review of the executive's decision-making. While the judiciary works as an important counterbalance, sealed cover proceedings and the seal on the confidentiality provisions contained in the Blocking Rules limit judicial capacity to conduct effective reviews of executive decisions. While the judiciary has established rules of transparency, the executive routinely hides behind claim of national security to avoid being subject to these requirements. In effect, there is an asymmetrical power imbalance where the executive is the gatekeeper and the judiciary only has the opportunity to intervene after harm has occurred. Furthermore, the executive's power to control content on the Internet has been further increased by the 2021 IT Rules, which require intermediaries to remove content in a short time frame. It is essential to strengthen the role of the judiciary in order to ensure that the administration does not infringe upon the digital rights of people and to ensure that the rule of law prevails over secretive governmental actions.

CONCLUSION

The subject of this research document is to analyze the state of internet censorship in India and the fine line that lies between state sovereignty versus individual digital freedom. The IT Act and the provision set out in Section 69A provide a framework for how to regulate internet content, yet there has been an increased amount of control being placed over OTT platforms and digital news. All signs point toward an increase in the amount of executive power controlling these platforms.

Rulings such as Shreya Singhal and Anuradha Bhasin have been critical in holding that the Fundamental Rights set forth in Article 19 also apply to online and digital communications; however, the ongoing use of internet shutdowns and the continued issuance of secretive blocking orders indicates judicial guidance is still being circumvented. The "Chilling Effect" is another major concern because vague "public order" justifications can deter people from filing complaints against the government or engaging in journalistic pursuits.

India must return to a legal system that encourages democracy by moving away from an environment of secretive administrative actions and towards one that embraces transparency and accountability. The appropriate application of the "Proportionality Test" is critical to ensuring that restrictive measures taken to limit access to information are a last resort rather than a

convenient means of suppression. Finally, maintaining the internet as an open mechanism for providing expression requires the continued use and application of independent regulatory reforms and the strength of the judiciary in overseeing how the law applies to institutions and individuals as they continue to evolve with technological advances. Thus, ensuring the law will continue to adapt to meet the needs of a changing digital world will ensure that digital governance does not become a vehicle for providing the government with unregulated access to surveillance of its citizens through internet usage.

BIBLIOGRAPHY

1. Constitutional Law of India – H.M. Seervai.

Authoritative commentary on Article 19(1)(a), reasonable restrictions, and judicial review.

2. Introduction to the Constitution of India – D.D. Basu.

Detailed explanation of free speech limits and constitutional safeguards.

3. Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Struck down Section 66A; clarified scope of Section 69A and intermediary liability.

4. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

Applied proportionality test to internet shutdowns; mandated publication of suspension orders.

5. Information Technology Act, 2000 (as amended in 2008).

Core statutory framework governing online censorship and blocking powers under Section 69A.

6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Introduced traceability mandates, three-tier grievance redressal, and digital news oversight.

7. Internet Freedom Foundation – Policy Briefs & Transparency Reports.

Empirical documentation of blocking orders, shutdown trends, and legal challenges.

8. Software Freedom Law Center, India – Internet Shutdown Tracker & Legal Analyses.

Provides verified data on frequency, legality, and economic cost of shutdowns in India.

9. Reporters Without Borders – World Press Freedom Index Reports (2023–2025).

Comparative analysis of India's digital press freedom environment.

10. UNESCO – Guidelines for the Governance of Digital Platforms (2023). International standards on content moderation, transparency, and safeguarding freedom of expression.

11. PRS Legislative Research – Legislative Briefs on IT Act Amendments & IT Rules 2021.

Objective summaries of statutory changes and regulatory implications.

12. The Wire – Investigative articles on Section 69A blocking orders and digital censorship practices. Explores secrecy in blocking procedures and executive expansion.

13. Journal - Censored Planet and the Open Observatory of Network Interference (OONI) provide ongoing technical measurements of censorship global.

14. Source: Tom's Guide
<https://share.google/xoWs34K46pok56xOE>,
 visited at 18:00 pm (23-02-2026)