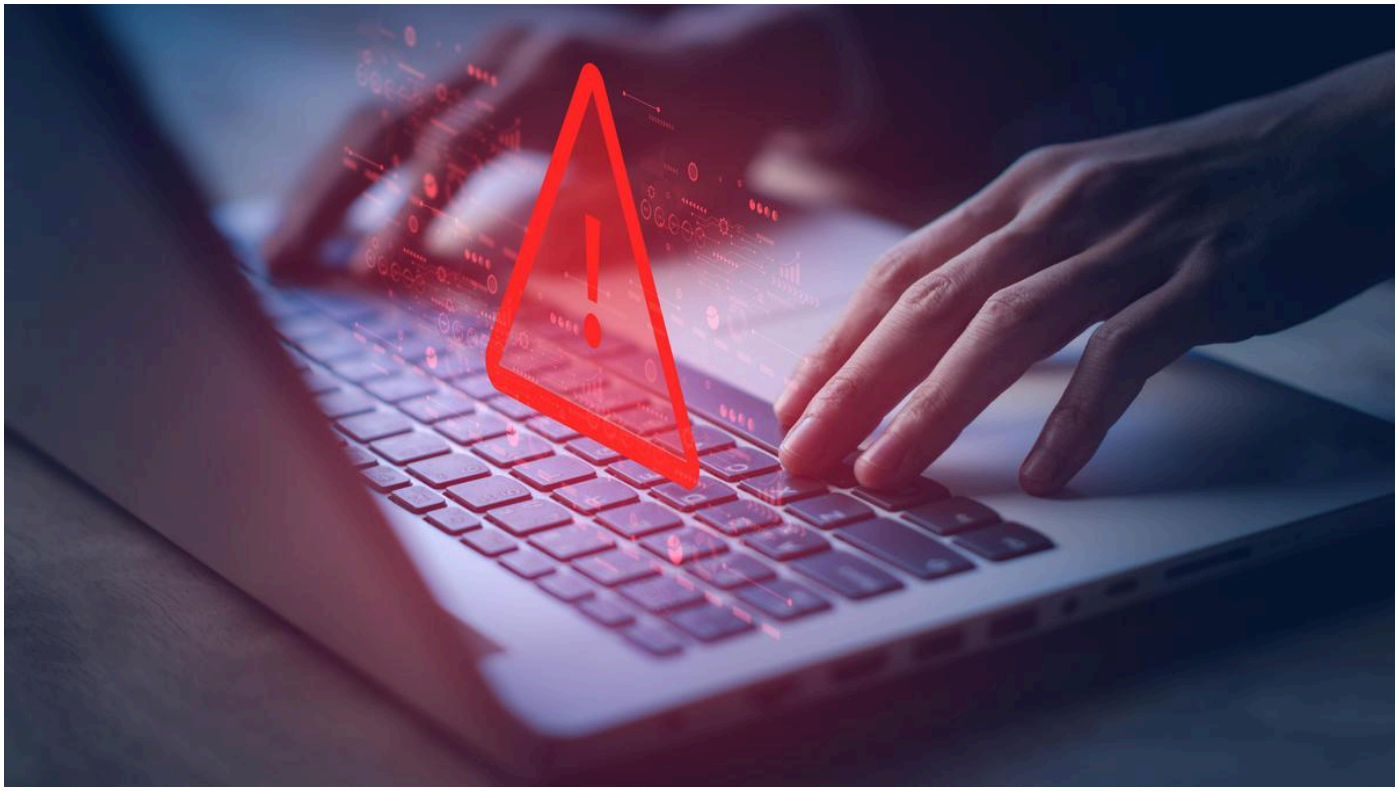
Understanding India's internet censorship regime

An internet user's experience in India depends on the ISP, which determines their access to content

Updated – April 07, 2026 08:42 am IST

KARAN SAINI



Representational image

The experience an Internet user has in India is closely tied to the Internet Service Provider (ISP) they choose. Perceived differences are not limited only to pricing and quality of service, but also to how much of the Internet a user can access, which changes from one ISP to another. This is because ISPs in India — much like everywhere else — block websites in response to government and court orders. However, implementation is not uniform across ISPs, and blocklists vary widely.

Sections 69A and 79 of the Information Technology Act, 2000, empower the government to issue blocking orders to ISPs and intermediaries. The licensing agreement for ISPs

explicitly requires that they "block Internet sites [...] as identified and directed by the Licensor from time to time." ISPs are confidentially bound to the blocking orders they receive and implement. In copyright and trademark dispute-related cases, blocking orders are made public as part of court orders. The blocking of websites usually only comes to light when users notice it is inaccessible and raise questions — such as what happened when Supabase was recently blocked. In some instances, the government may choose to announce its blocking actions, such as when it announced the blocking of 59 Chinese applications including TikTok in 2020.

Protocols and implementation

The Internet is made up of protocols like the Hypertext Transfer Protocol (HTTP), Transport Layer Security (TLS), and Domain Name System (DNS) among others. When an ISP receives a blocking order, it is free to implement it through any or all of these protocols. DNS is the first layer a user interacts with when trying to access a website and is responsible for translating names like example.com to addresses that browsers can understand. When an ISP wants to block a domain at the DNS layer, it configures its servers to return a false answer. This technique is called DNS poisoning. A user's request for example.com doesn't end up at the actual address for the website, but to whatever address the ISP has pointed it to instead.

ISPs can also intercept unencrypted HTTP traffic and return a block page, though this technique is largely outdated as most websites and browsers now use HTTPS by default. For HTTPS websites, ISPs look for the Server Name Indication (SNI) field to identify and drop connections to blocked domains before they are established. In practice, Most Indian ISPs rely primarily on DNS blocking as it is cheap to implement and requires no deep packet inspection.

What the data shows

To understand the scale of website blocking in India, I queried the DNS servers of six major and regional ISPs to test the censorship of 294 million domains, representing nearly the entire visible domain name space. These tests were carried out over many months in 2025 and contribute to the largest study of DNS-level website blocking in India to date. The study quantifies what previous qualitative research on Internet censorship in India has shown. Despite receiving the same blocking orders, not all ISPs block the same websites.

Out of the total 43,083 blocked domain names found by the study, only 1,414 were blocked by all six ISPs. This is caveated by the fact that some of the ISPs surveyed may be using other abovementioned protocols to block these domains, which the study does not cover. What is clear however is that at least on the DNS layer, domains are treated inconsistently based on the category of content they host. Piracy, peer-to-peer file sharing, pornography and gambling websites make up the majority of what is blocked, yet blocks are not consistently enforced across ISPs. For domains hosting terrorism and militancy content, blocking consistency across ISPs goes up dramatically. Perfect consensus can be seen in certain sensitive cases, such as the blocking of China's Weibo.com or the website of Srinagar-based publication The Kashmir Walla, showing that some orders are treated more seriously than others. Along with this, almost all ISPs appear to engage in arbitrary blocking in some form.

While highlighting only some notable blocks, the study shows the haphazard way in which both regional and national ISPs are currently implementing blocking orders. In the absence of a standardised framework or guidelines, ISPs are left to their own devices, resulting in an inconsistent blocking landscape. A domain blocked by one provider may be freely accessible through another, undermining the stated rationale for blocking while still infringing on the rights of users served by the more aggressive ISP. Domains officially ordered unblocked continue to remain blocked by some ISPs in clear defiance of orders, but without penalty to ISPs or respite for operators of such websites.

Inconsistency is not the only problem however. The regime is needlessly opaque. An ideal system would see disclosure of blocked domains from the source, with exceptions only for sensitive matters such as those concerning national security and websites hosting child sexual abuse material. A perfect example of this is the many malicious domains found blocked by the study, which is arguably in the public interest, but which cannot be distinguished from overreach without disclosure. The Supreme Court in *Shreya Singhal vs. Union of India* (2015) upheld Section 69A but emphasised procedural safeguards, including a review committee and the right of affected parties to be heard. In practice, neither can operate meaningfully as long as the system runs like patchwork.

(Karan Saini is an independent security researcher from New Delhi., and the author of the "Poisoned Wells" report)

Published – April 07, 2026 08:30 am IST