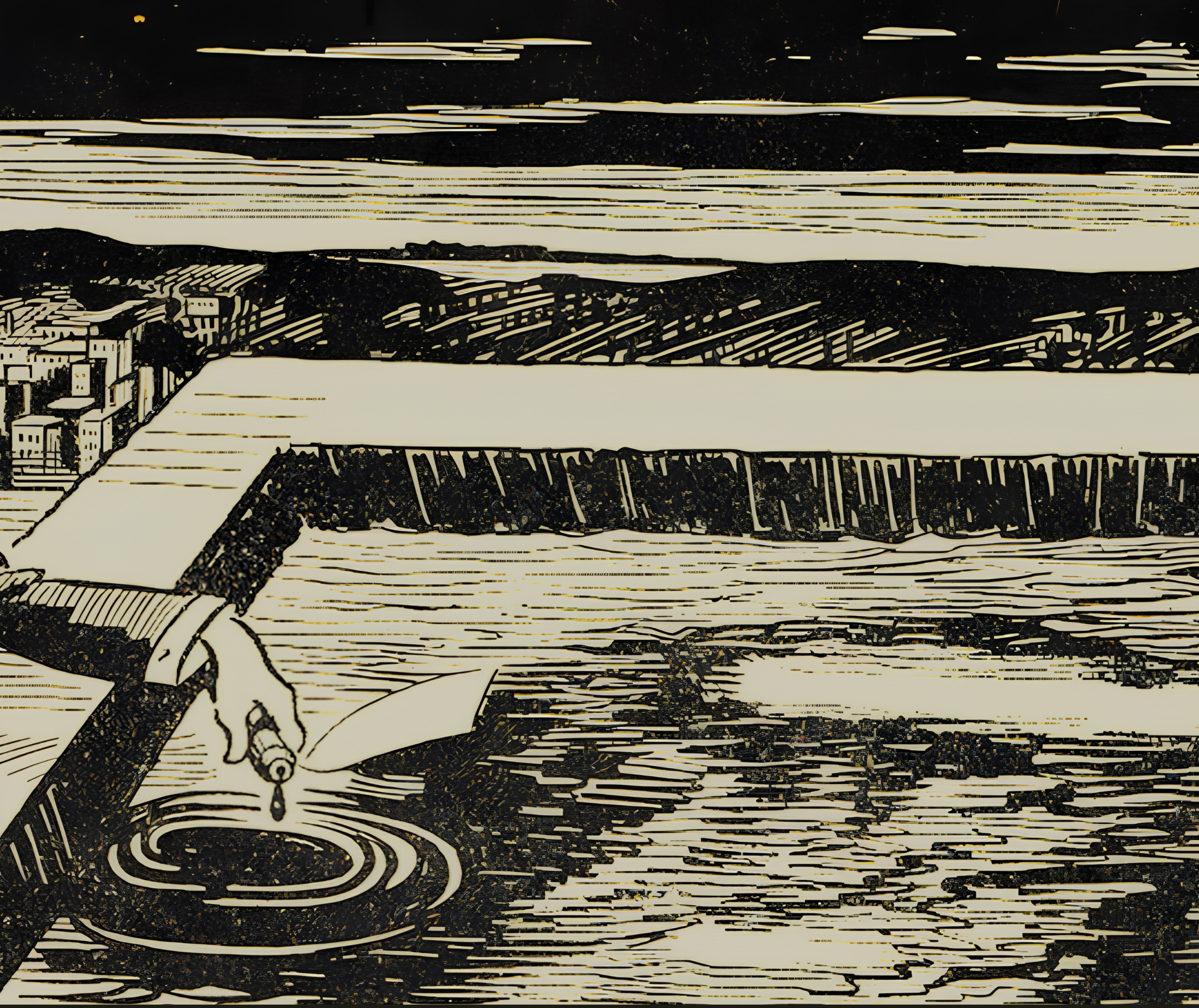


Poisoned Wells

Examining the scale of DNS censorship in India

Karan Saini

Executive Summary

While some internet service providers (ISPs) have started to use more sophisticated techniques to implement web censorship, Domain Name System (DNS) filtering continues to remain a popular method for both small and large Indian ISPs. This report presents findings from the largest study to date of DNS-based censorship in India. The point-in-time study collected DNS measurements for 294 million registered apex (root-level) domains across six Indian ISPs, sending 1.76 billion DNS queries in total. Its findings offer censorship circumvention tool developers and internet freedom researchers important insights and avenues for further investigation.

Key findings:

- A total of 43,083 unique apex domains were confirmed blocked via DNS filtering — a sixfold increase over the previous largest study (which documented 6,787 blocked domains).
- A major ISP's misconfiguration of a blocking rule is causing significant overblocking where an entire global top-level domain (.yokohama) is inaccessible.
- Only 9,363 censored domains (21.73% of the blocklist produced by this study) had ranks in the Tranco list (a reliable and transparent top-sites ranking list), demonstrating that test lists drawing from popularity rankings do not accurately represent censorship scale.
- There is aggressive blocking of services and platforms across categories including business, hosting, research, and communication.
- A state-owned, public-sector undertaking (PSU) ISP's consumer blocklist is hypothesized to be derived from filtering policies intended for government offices.

Recommendations for the internet freedom community:

- Developers of tools that rely on name resolution should consider configuring DNS over HTTPS (DoH) by-default regardless of system locale, but especially in regions where DNS queries are known to be filtered.
- Certain jurisdictions regulate VPN and cloud infrastructure providers, but not the use of general network utility software, which could be designed to enable censorship circumvention without relying on external networks.
- Tool developers and other members of the internet freedom community should consider developing and promoting network utility tools that enable censorship circumvention without anonymizing traffic or relying on external network infrastructure.

Table of Contents

01

Background

Indian internet landscape

India has an official population of 1.46 billion and nearly 1 billion internet subscribers as of September 2025. Despite a diverse market composition, consumer internet services in the country are dominated by a handful of players. The top five ISPs serve around 98.51% of internet subscribers in the country. Wireless broadband services are more popular than wired internet.

Service provider	Market share (%)	Study coverage
Reliance Jio Infocomm Ltd.	50.77%	Y
Bharti Airtel Ltd.	31.18%	Y
Vodafone Idea Ltd.	12.83%	N
Bharat Sanchar Nigam Ltd.	3.49%	N
Atria Convergence Technologies	0.24%	Y

Table 1: Top five broadband (wired + wireless) service providers by market share as on 30th September 2025 (source: Telecom Regulatory Authority of India, Telecom Subscription Data for September 2025).

Legal framework

Section 69A and Section 79 of the Information Technology Act form the legal framework that allows the state to censor information on the internet. The Central Government and the courts have the power to issue blocking orders to internet and telecommunications service providers, as well as takedown orders to online platforms.

According to a report by the Software Freedom Law Centre, India, 55,607 Uniform Resource Locators (URLs) were ordered to be blocked between the years 2015 and 2022. Blocking orders are confidential. In specific cases, when courts order the blocking of websites or applications, the blocking orders are made public. This has been restricted to cases of intellectual property disputes and trademark violations. In specific cases, the state may choose to announce certain blocking actions.

Filtering techniques

The legal framework for censorship does not mandate any specific traffic filtering mechanisms. ISPs are free to choose and implement traffic filtering mechanisms according to their own technical abilities and operational needs. A direct consequence has been that users perceive and experience website blocking inconsistently depending on their choice of ISP.

Censorship technique	Description
HTTP-based	This involves inspecting unencrypted Hypertext Transfer Protocol (HTTP) traffic, typically monitoring elements like the HOST header field (which reveals the website identity) in plaintext HTTP requests. Upon detection, the ISP can respond with a forged success message often containing a statutory censorship notification (a block page), disrupt or drop the connection, or send a TCP RST (reset) packet to force client disconnection.
DNS-based	This method involves manipulating the Domain Name System (DNS) resolution process. Techniques include DNS poisoning (returning an incorrect or “bogon” IP address maintained on the ISP’s DNS servers) or DNS injection (intercepting a plaintext DNS query and injecting a false response).

Censorship technique	Description
SNI-based TLS blocking	This technique exploits the unencrypted Server Name Indication (SNI) field in the TLS (Transport Layer Security) ClientHello message during an HTTPS handshake, which carries the destination hostname in plaintext. Upon detecting a blocked domain name, the ISP intercepts the connection and drops or terminates it, often by sending a TCP reset packet.
IP/TCP-based	Blocking connections based strictly on the IP address or transport layer protocol headers (like destination port numbers).

Table 2: Web censorship techniques

Research gap

Earlier research on India's web censorship apparatus has primarily attempted to investigate and document the filtering techniques used by various regional and national ISPs. Such studies tested only a few thousand domains, at most, and relied on curated lists of potentially blocked websites to study censorship. This study focuses instead on ascertaining the scale of DNS-based web censorship, as it is a censorship technique widely employed by both small and large Indian ISPs.

02

Methodology

Research questions

The study was designed to answer the following questions:

1. How many domains are censored using DNS filtering in India?
2. Is there consensus among ISPs on which domains to censor?
3. Is there overblocking?
4. If yes, is it caused by misconfigurations? What specific rules trigger overblocking?

Test list construction

The test list was compiled from two sources:

ICANN's Centralized Zone Data Service (CZDS) Platform:
Zone files from participating generic top-level domains (gTLDs) were accessed using the czds tool by lanrat. A Bash script was used to extract all domains from the zone files, yielding 221,494,493 unique apex domains. This source has a limitation in that it does not provide coverage of country-code TLDs (ccTLDs).

Domains Project:
The other source was the Active Domains list from March 2025, which contains 1.3 billion domains (including subdomains). This list contains only domains that are considered "live." The Python library `tldextract` was used to extract apex domains, yielding 231,394,238 unique entries.

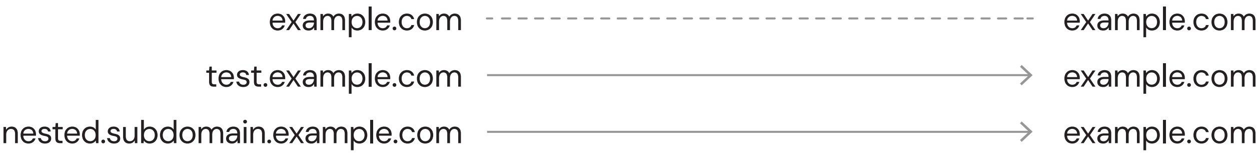


Figure 1: Extraction of apex domains

After combining both sources and performing a deduplication step, the final test list contained 294,480,735 unique apex domains.

ISP selection

Six ISPs were selected based on their market share, known use of DNS filtering, and geographic diversity.

ISP	ASN	Service area
Reliance Jio Infocomm (Jio) *	AS55836	National
Bharti Airtel (Airtel) *	AS9498	National
Atria Convergence Technologies (ACT) *	AS18209	Major cities throughout the country
Mahanagar Telephone Nigam Ltd. (MTNL)	AS17813	Delhi and Mumbai
You Broadband	AS18207	State of Maharashtra
Quadrant Televentures (Connect Broadband)	AS17917	State of Punjab

Table 3: ISP coverage

*These ISPs have more than one Autonomous System Number (ASN) assigned. The study looked only at the ASNs mentioned above.

Measurement collection

Direct connections: New internet connections were acquired for Jio, Airtel, and ACT. Dedicated machines with 1 Gbps ethernet ports were set up for each ISP at a single location.

Remote measurements: For You Broadband, Connect Broadband, and MTNL, infrastructural DNS resolvers belonging to these ISPs that were misconfigured and accepted DNS queries from outside their networks were identified and used. Three separate virtual machines were leased from a leading cloud service provider to collect remote measurements.

The methodology for identifying infrastructural resolvers involved:

- Leveraging data from Censys (which appropriately labels forwarding and recursive DNS resolvers) and Shodan.
- Performing reverse hostname lookups to validate that DNS resolvers were part of ISP infrastructure.
- Manual verification to avoid misclassifying residential or institutional DNS resolvers as infrastructural resolvers.

Tools

ZDNS: Open source tool and framework for collecting large-scale DNS measurements. `ZDNS` was used instead of `massdns` due to its performance advantages and continued active development.

blockbust: A Python tool was created that wraps around `ZDNS` and provides utilities to help detect DNS censorship. `blockbust` generates configuration files for networks, including detected blocking signatures. It simplifies blocklist building by processing collected measurements and extracting censored domains.

Parameters

Query type: Queries were limited to the DNS `A` record type.

Rate limiting: A queries per second (QPS) rate of ~100 was used. This rate was achieved by modifying the number of threads in use, since `ZDNS` does not have a built-in switch for limiting queries.

Censorship detection

The method for labelling a site as censored involved establishing the blocking signature used by an ISP. This was done by first querying a popularly censored, non-geo-DNS domain (e.g., `thepiratebay.org`) using a third-party DNS service provider to establish the baseline response, and then querying the same domain using an ISP DNS resolver, where the deviation was considered the ISP's blocking signature.

Blocking signatures can manifest as:

- public IP addresses — sometimes within the same AS as the censored network, sometimes within cloud service provider networks;
- private IP addresses or loopback addresses; or
- non-existent domain (`NXDOMAIN`) responses.

Control measurements were collected for domains suspected of being blocked through a third-party DNS resolver (which is assumed to be uncensored).

Control measurements were collected for both `A` and `NS` DNS record types.

Ethical considerations

The research was guided by the following principles:

Avoid degrading service: Direct and remote measurement collection was limited to a reasonably low QPS rate.

Use attributable ISP infrastructure for remote measurements: To avoid potential legal consequences for organizations or individual users, only resolvers attributable as being part of ISP infrastructure were used.

Address patently illegal content: In the output produced by this research, domains believed to contain patently illegal content (e.g., child sexual abuse material) were reported to appropriate authorities and adequately obscured in released data.

03

Results

Measurement scale

In total, 1,766,884,527 (1.76 billion) DNS queries were sent.

Query results:

- 1,544,458,209 (87.41%) returned `NOERROR`
- 60,503,716 (3.42%) returned `NXDOMAIN`
- 34,960,932 (1.98%) returned `SERVFAIL` (server failure)
- 3,661,598 (0.21%) returned `REFUSED`
- 123,300,072 (6.98%) failed for other reasons (e.g., `TIMEOUT`)

The number of unique domains with at least one successful measurement (`NOERROR` + `NXDOMAIN`) was 286,087,337. The number of unique domains with at least one `NOERROR` response was 281,045,732.

Blocked domain counts by ISP

ISP	# of blocked domains
Jio	15,245
Airtel	27,649
ACT	14,173
MTNL	20,085
You Broadband	14,052 (3 false positives removed)
Connect Broadband	9,414
Total (deduplicated)	**43,083**

Table 4: Blocked domain counts by ISP

Blocking signatures

ISP	Signature
Jio	`A` record pointing to 49.44.79.236
Airtel	`CNAME` record pointing to `dotblocking.dummy` (which has an A record pointing to 13.127.247.216)
ACT	`A` record pointing to 49.205.171.201 (resolver) or 49.207.46.62 (injection)
MTNL	`A` record pointing to 59.185.3.14
You Broadband	`A` record pointing to 203.109.71.154 and `NS` records pointing to ns[1-4].youbroadband.in
Connect Broadband	`A` record pointing to 202.164.51.25

Table 5: ISP blocking signatures

DNS filtering implementation findings

DNS injection: Out of Jio, Airtel, and ACT, only ACT performed DNS response injection. The injection was discerned by querying a collection of blocked domains against a server IP known not to be a DNS resolver. Any response in this scenario is indicative of DNS injection.

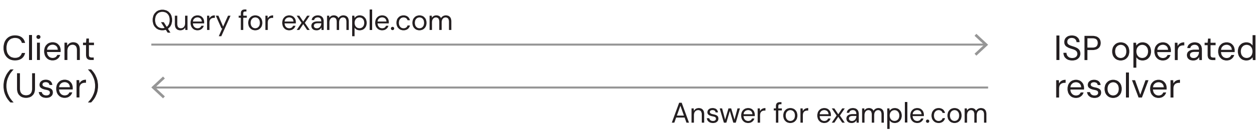


Figure 2: Regular DNS query (simplified)

Of the 14,173 domains censored by ACT, injection occurred consistently for 12,560 (88.6%) censored domains. The 1,613 domains for which injection did not occur did not overwhelmingly exhibit a pattern or belong to a particular TLD, though this should be investigated further.

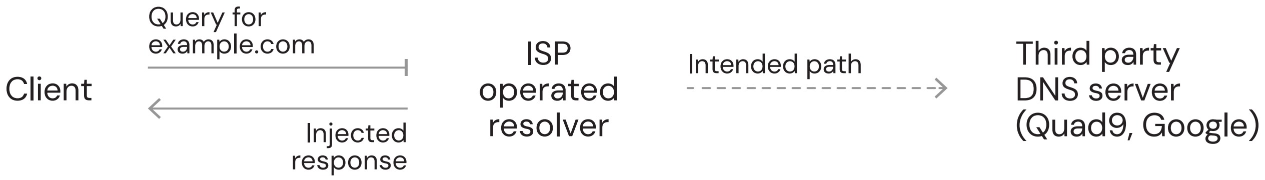


Figure 3: DNS injection (simplified)

Circumventing injection: It was possible to bypass the DNS response injection performed by ACT by communicating with a name server running on a non-standard port. Querying the Quad9 DNS server (9.9.9.9) on port 53 triggered injection, while querying the same server on port 9953 did not.

Censoring expired domains: Through secondary measurement collection, the study found that all ISPs continued to censor domains present in their blocklists even when the underlying domain no longer existed (i.e., expired domain registration.) This should be investigated further.

DNSSEC implementation: Jio, Airtel, ACT, and Connect Broadband implemented Domain Name System Security Extensions (DNSSEC) — a set of extensions to the DNS protocol for cryptographic validation of DNS records — at least partially, whereas MTNL and You Broadband did not. The impact of DNSSEC-related `SERVFAIL` responses in collected measurements is explored in the limitations section.

ISP	SERVFAIL	DNSSEC
Jio	6,128,852	Y
Airtel	4,878,299	Y
ACT	9,521,575	Y
MTNL	5,893,039	N
You Broadband	1,578,121	N
Connect Broadband	6,961,046	Y

Table 6: `SERVFAIL` responses and DNSSEC status

Data from APNIC about DNSSEC validation across Indian ASNs confirms the study's observations about DNSSEC implementation by the ISPs mentioned.

Misconfigured resolvers: The DNS resolvers for Connect Broadband and You Broadband sometimes provided additional data even when not explicitly requested. This misconfiguration allowed for the observation of nameservers configured for some successfully queried domains. While not a focus of this analysis, the additional data could be useful to analyze the blocking of authoritative nameservers.

False positives: Three domains were present in the blocklist generated for You Broadband: nirma.com, youbroadband.in, and youwifi.in. Control measurements revealed that nameservers for these domains coincided with the discerned blocking signature for You Broadband. These domains were removed from the blocklist.

Domain categorization

Domain categories were classified using a mixed approach. Manual classifications based on search engine meta-descriptions were supplemented by open source category-specific lists maintained for network security and adblocking tools, along with machine-learning aided classification. An ensemble of models was used for the machine learning approach. The classification relied on a modified version of the test list taxonomy by Citizen Lab. The full classification taxonomy is provided in the appendix.

Top 15 Domain Categories

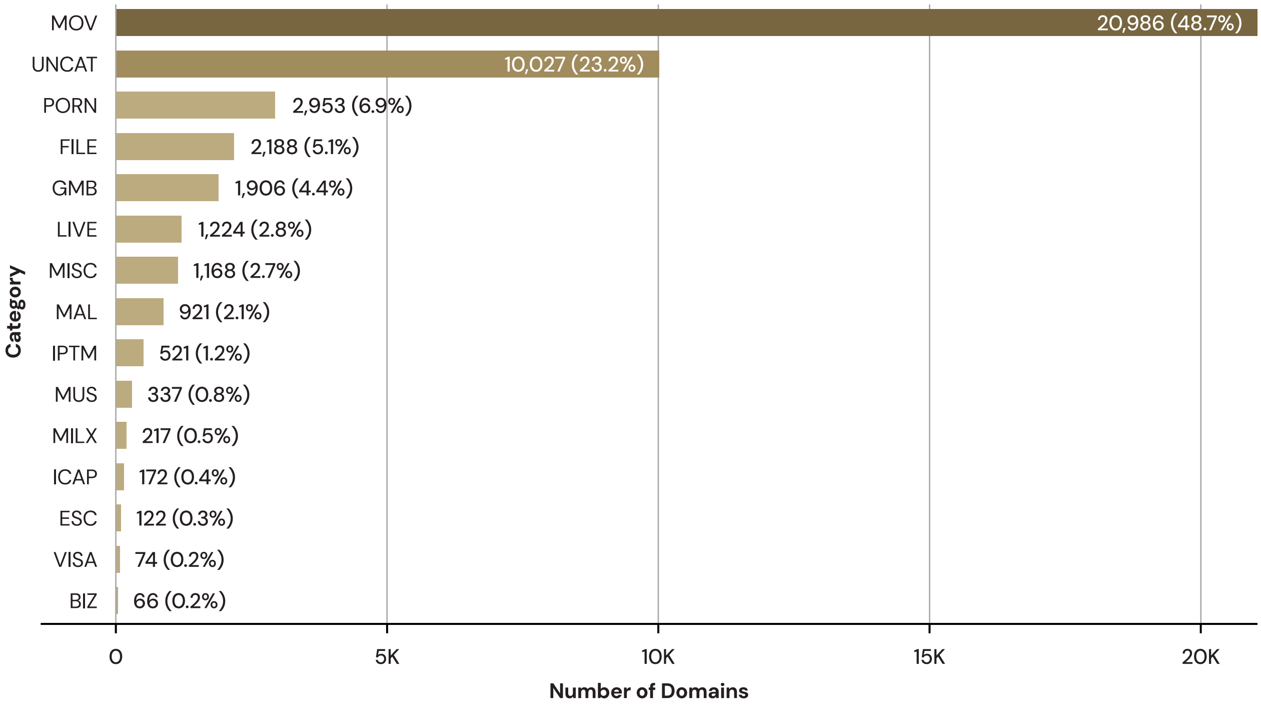


Figure 4: Top 15 domain categories in the compiled blocklist

Blocking consensus across categories

To analyze consensus, the blocklist was filtered to only include domains with successful measurements from all six ISPs. Analysis of 32,451 domains (75.32% of the 43,083-domain blocklist) revealed significant variations in blocking consensus.

Category	Domains	% of filtered blocklist	Universal blocking rate
MOV	16,752	51.6%	4.54%
PORN	2,071	6.38%	0.53%
FILE	1,795	5.53%	8.86%
GMB	1,269	3.91%	13.48%
MILX	171	0.53%	38.60%

Table 7: Blocking consensus across five categories in the filtered blocklist

Movie and TV piracy (MOV) domains comprised the majority of the filtered blocklist at 51.62%, yet showed minimal universal blocking (4.54%). In contrast, the terrorism and militants category (MILX), despite comprising only 0.53% of the filtered blocklist, showed the highest consensus, with 38.60% of domains blocked by all six ISPs.

Gambling (GMB) domains showed moderate universal blocking consensus (13.48%), whereas pornography (PORN) domains, despite comprising 6.38% of the filtered blocklist, showed only 0.53% universal blocking — illustrating highly inconsistent treatment of pornographic content across ISPs.

Popularity of blocked domains

Tranco is a reliable and transparent top sites ranking list. The full Tranco list (generated on March 6, 2025) was used to enrich the compiled blocklist. Only 9,363 (21.73%) domains from the compiled blocklist had ranks in the Tranco list.

Analysis

Jio's interpretation of the TikTok blocking order: On June 29, 2020, the Ministry of Information Technology announced the blocking of 59 apps "prejudicial to sovereignty and integrity of India," including TikTok, which was removed from app stores. TikTok also made its own services inaccessible to users located in India.

Jio blocks not only the main TikTok domain but also the TikTok CDN domain (tiktokcdn.com, Tranco rank #28), as well as the video service domain (tiktokv.com, Tranco rank #67). This represents a wider implementation of the blocking order than other ISPs.

While the actual blocking order sent to ISPs is not available publicly, the fact that only Jio blocks TikTok's infrastructure domains could suggest that:

1. Jio implemented a broader interpretation of the blocking order; or
2. the order specified these domains but other ISPs are non-compliant, or are using other techniques to block these domains.

Additionally, Jio is the only ISP blocking:

- uol.com.br (Tranco rank #496) — Brazil's largest content and technology company
- umeng.com (Tranco rank #956) — a Chinese mobile analytics company

Document and research sharing websites blocked by You Broadband:
You Broadband uniquely blocks three major document sharing services:

Domain	Tranco rank
slideshare.net	#317
scribd.com	#486
academia.edu	#842

Table 8: Three major document and research sharing services exclusively blocked by You Broadband

All three platforms allow users to upload and share documents. Academia.edu focuses on academic research papers, Scribd is used for general document sharing, and SlideShare specializes in presentations.

Airtel's blocking of an entire gTLD: Airtel is the most aggressive ISP in terms of number of domains blocked. It blocks the entirety of the `.yokohama` gTLD, which the author hypothesizes is caused by a misconfiguration. The blocking rule behind this was secondarily verified by querying non-existent domains within the gTLD.

Domain	Description
*.yokohama	~3,000 domains in the test list
dailymotion.com	Video sharing platform, Tranco rank #347
is.gd	URL shortener, Tranco rank #3485

Table 9: Examples of domains exclusively blocked by Airtel

Airtel was first reported to block DailyMotion in 2012 following a court order over copyright infringement. The government ordered the site blocked again in 2015, then reversed the decision shortly after. It is not known when is.gd was first blocked.

MTNL's blocking of popular services: MTNL blocks a variety of popular domains across categories.

Domain	Description
t.me, telegram.org	Telegram messaging, Tranco ranks #116 and #438
discord.com	Gaming/community platform, Tranco rank #251
slack.com	Business communication tool, Tranco rank #250

Table 10: Communication and messaging platforms exclusively blocked by MTNL

Domain	Description
bit.ly	URL shortener, Tranco rank #71
lencr.org	Let's Encrypt certificate authority, Tranco rank #159
ax-msedge.net	Microsoft CDN, Tranco rank #62

Table 11: Infrastructure services exclusively blocked by MTNL

Domain	Description
dropboxapi.com	Dropbox API, Tranco rank #1229
mega.co.nz	File storage platform, Tranco rank #464

Table 12: File sharing services exclusively blocked by MTNL

Domain	Description
behance.net	Adobe portfolio platform, Tranco rank #473
freshchat.com	Customer messaging platform, Tranco rank #4456
ip-api.com	IP address geolocation API, Tranco rank #923
zedge.net	Ringtone/wallpaper platform, Tranco rank #7028

Table 13: Other notable services exclusively blocked by MTNL

Blocking of a numeric pattern: MTNL uniquely blocks a set of domains beginning with the numeric pattern “1004.” Supplementary measurements were not collected to verify whether these blocks were caused by a misconfigured regular expression-based blocking rule.

10041do1m.com	1004bridge.com
1004airport.com	1004bulbolrak.com
1004baendaengi.com	1004byeongeo.com

Table 14: Examples of domains blocked by MTNL with the ‘1004’ pattern

MTNL also uniquely blocks several Internationalized Domain Names (IDNs) in the Korean language (Hangul script). It is also unclear whether these blocks are intentional or caused by a misconfigured regular expression-based rule for domains beginning with "`xn--`" — which is how non-Latin scripts are denoted in ASCII-compatible encoding (Punycode) — as supplementary measurements were not collected. It is important to note that MTNL does not indiscriminately block all IDN domains with non-Latin scripts, nor all domains with the "`xn--`" prefix.

Domain	Punycode representation
다지음서울.com	xn--2j1br3ydle4qa91h.com
섬깡다리축제.com	xn--2l0bp9f22gmli23ifqi.com
올벼쌀.com	xn--2l3bq8itxc.com
섬망둥어축제.com	xn--2u1bs7hm8gw2e9pdful.com
정훈테크.com	xn--2y5bo6mgtaf4o.com
베리트디자인.com	xn--2z1b30g1ycl6podw85e.com

Table 15: Examples of domains blocked by MTNL in the Korean language (Hangul script)

What explains MTNL's arbitrary blocking behaviors? Apart from being a consumer internet services provider in the cities of New Delhi and Mumbai, MTNL is also popularly used within ministries, departments, and other government undertakings.

In June 2025, the Department of Telecommunications (DoT) urged state governments to use the services of MTNL and Bharat Sanchar Nigam Limited — another state-owned PSU ISP — citing security concerns with privately owned service providers. Keeping in mind the possibility of arbitrary overblocking, the author hypothesizes that MTNL's consumer blocklist includes domains that are supposed to be restricted only within government offices.

Multiple ISPs block domain registrars: These blocks could potentially be related to the Delhi High Court observation that domain registrars were not complying with judicial orders. “We can’t change the international system but if you operate in India, we will ask you to follow certain (norms). We will tell MEITY (Ministry of Electronics and Information Technology) to block the DNR (domain name registrar) if you don’t comply.”

Domain	Blocked by
Afternic.com	Airtel
BuyDomains.com	ACT, You Broadband
Squarespace.net	MTNL
njal.la, njalla.do	MTNL

Table 16: Examples of domain registrars blocked by ISPs

VideoLAN continues to be blocked by ACT despite unblocking order: MEITY ordered the unblocking of the domain for VideoLAN (the organization behind VLC Media Player) in 2022. Despite an official unblocking order, ACT continues to block the videolan.org domain as of this study.

Blocking of government domains: The National Informatics Centre (NIC), MEITY, oversees the `nic.in` and `gov.in` domain zones. Despite this, two `gov.in` domains were found in the compiled blocklist.

Domain	Description	Blocked by
mes.gov.in	Current domain for the website of the Military Engineer Services, Corps of Engineers of the Indian Army	You Broadband
rera-punjab.gov.in	Domain previously used for the website of the Real Estate Regulatory Authority of the State of Punjab	Connect Broadband

Table 17: Blocked domains in the gov.in zone

Blocking of anonymization tools: Domains in the anonymization and circumvention (ANON) category were found to be blocked across multiple ISPs. MTNL exclusively blocked the domains of at least two popular VPN services, including Surfshark (surfshark.com, Tranco rank #1048) and AdGuard VPN (adguard-vpn.online, Tranco rank #1601). You Broadband exclusively blocked domains for Urban VPN (urban-vpn.com, Tranco rank #4279) and the VPN Gate (vpngate.net, Tranco rank #46554) service. Airtel was found to block UltraVPN (ultravpn.com, Tranco rank #194201).

Blocking of media domains: The domain for Asian News International (aninews.in, Tranco rank #27923), India's largest newswire service, was exclusively blocked by You Broadband. The domain for The Kashmir Walla (thekashmirwalla.com, Tranco rank #1280750), an independent news and opinion website based in Srinagar, India, was blocked by all six ISPs in this study (MEITY ordered the blocking of this domain in 2023).

05

Comparison with previous studies

Study (year)	Domains confirmed blocked	Notes
Yadav et al. (2018)	N/A	Maximum 483 sites by a single ISP (Vodafone) via HTTP filtering
Singh et al. (2020)	4,033	Largest known corpus at that time
Katira et al. (2023)	6,787	Across 71 autonomous systems
This study (2026)	43,083	DNS filtering only; sixfold increase in blocklist size

Table 18: Comparison with previous India-specific censorship research

06

Limitations

Methodological limitations

Protocol coverage: The methodology addresses only DNS filtering. Other techniques like HTTP host header-based filtering or Server Name Indication (SNI) inspection-based Transport Layer Security (TLS) filtering were not considered. Due to how DNS works, only blocking at the domain level was captured. Censorship of specific web pages within a domain could not be discerned.

DNSSEC: Several ISPs implemented DNSSEC, but the methodology for this study was not designed to distinguish whether `SERVFAIL` responses were due to server failures or failed DNSSEC validation potentially caused by underlying censorship.

False negatives: False negatives may be possible in `NOERROR` responses if there is more than one simultaneous blocking signature per network, in `SERVFAIL` responses if the ISP is using DNSSEC, and in `TIMEOUT` and `ERROR` responses since those domains were not successfully queried.

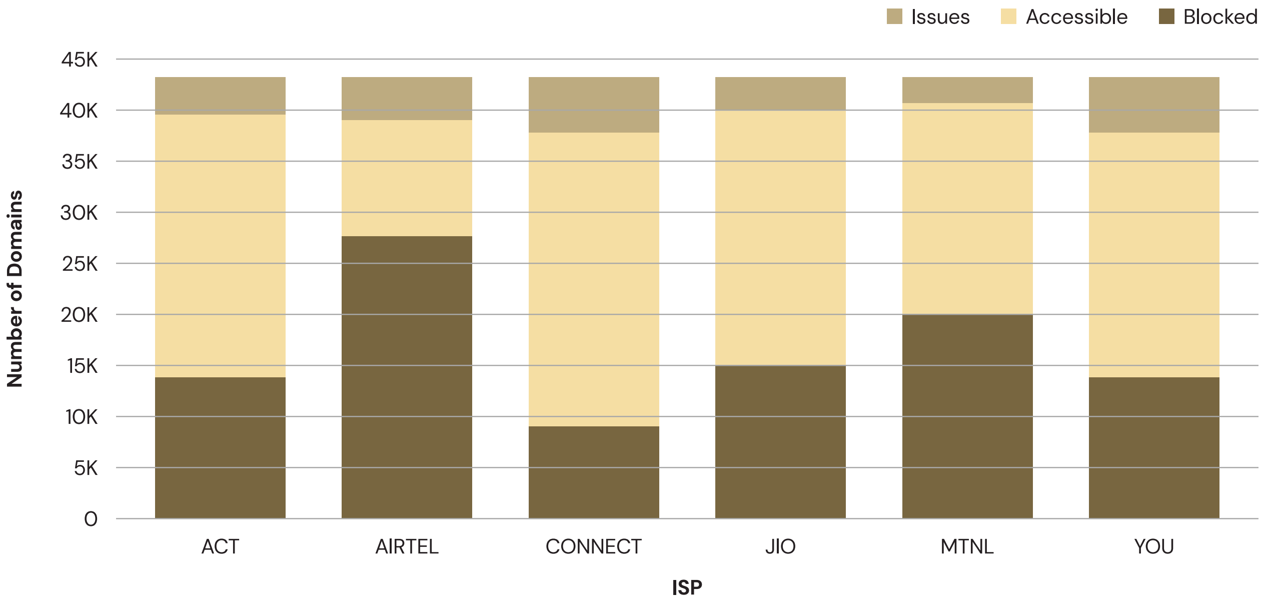


Figure 5: Data quality for compiled blocklist

Measurement interruptions: The measurement collection process faced several interruptions due to utility and internet service outages, and technical errors. Apart from MTNL, all ISPs faced interruptions during the measurement collection process. When resuming measurements, a small number of domains that were present in the `ZDNS` program's memory but which had not been queried, were omitted.

Protocol awareness: Jio, the largest ISP by market share, blocks fewer domains using DNS filtering than MTNL. This, however, does not mean that Jio is a less censorious network, as prior research showed that Jio uses a variety of censorship techniques in conjunction — including SNI inspection-based TLS blocking. This study, including the analysis, is limited in its scope and visibility to the DNS protocol.

Test list limitations

No .ru ccTLD domains: The Active Domains list from the Domains Project did not contain any `.ru` domains. According to cctld.ru, the number of "active" `.ru` domains at the time of measurement collection was 5,836,058. The `.ru` ccTLD featured at number eight in a list of "most abused" TLDs by SURBL at the time of measurement collection.

Blocking of subdomains: Subdomains were stripped from the test list in order to make measurement collection feasible. Supplemental measurements were not collected to test blocking conditions for subdomains. As a result, there is no visibility of blocked subdomains.

Temporal limitations

Point-in-time: This study serves as a point-in-time exercise and does not answer questions that require measuring censorship continually.

Synchronicity: Measurement collection across ISPs did not begin and conclude at the same time due to technical limitations.

ISP	First measurement	Last measurement
ACT	2025-03-09	2025-04-01
Jio	2025-03-09	2025-03-29
Airtel	2025-03-11	2025-04-10
MTNL	2025-04-12	2025-05-23
You Broadband	2025-04-21	2025-09-09
Connect Broadband	2025-04-22	2025-06-17

Table 19: Measurement collection timeline

The longer measurement period for You Broadband was caused by quality of service and technical issues.

Classification limitations

Website categorization is inherently subjective. The classification process undertaken was therefore best-effort in nature. As a result, the compiled blocklist may contain both categorical overlaps and potential misclassifications.

07 Discussion

Changes in blocking signatures

Compared with data from CensorWatch, the forged IP addresses used for DNS censorship by some ISPs have changed. The reason behind these changes is not immediately clear and should be investigated further. At the same time, some ISPs' blocking signatures have not evolved. You Broadband was using the same IP address at the time of measurement collection for CensorWatch as it is at the time of writing. MTNL has been returning the same IP address for blocked websites since 2015.

Technical observations

While some ISPs have started to move to more sophisticated techniques to implement censorship, DNS filtering continues to remain a popular censorship technique for both small and large Indian ISPs.

Recommendations for developers and operators

A significant portion of web censorship in India relies on DNS filtering. Developers of tools that rely on name resolution (such as web browsers) should consider configuring DNS over HTTPS (DoH) by-default regardless of system locale, but especially in regions where DNS queries are known to be filtered.

DNS service providers should consider additionally operating on non-standard ports. The research found that DNS injection performed by ACT only occurred on port 53, the standard port for DNS traffic. DNS queries sent via other ports were not subject to filtering. At the time of writing, only one popular DNS service provider (Quad9) was found to additionally operate their DNS server on a non-standard port.

08

Future work

DNS filtering research

Blocking of subdomains: Future research could test blocking behavior for subdomains specifically using apex domains already known to be blocked.

Investigating DNSSEC-related failures: Future research should incorporate DNSSEC validation to account for `SERVFAIL` responses that might be caused by underlying censorship.

Multi-protocol research

Testing censorship via other protocols at scale is necessary to assess the overall censorship practices of ISPs, especially in regions with federated information controls like India, though this would not be without challenges. While it may be unfeasible for continuous global network interference and censorship detection platforms to test censorship across multiple protocols for every visible domain, point-in-time exercises like this study could provide useful snapshots for understanding ground truth.

Other research directions

Blocking of mobile applications: Apart from blocking websites, the state also issues orders to app stores to take applications down or make them inaccessible. Research could correlate announced app blocks to test censorship of their associated domains.

Platform censorship: Globally, censorship is increasingly moving to platforms like YouTube, X, and Meta. Developing metrics and techniques to measure censorship on platforms reliably is an interesting research angle.

09

Conclusion

This report presents the largest study of DNS censorship in India till date, both in terms of test list coverage as well as the size of blocklist produced. The study tested 294 million domains across six ISPs representing approximately 82% of internet subscribers in the country, identifying 43,083 blocked apex domains. The compiled blocklist produced by this study represents a sixfold increase over the previous largest censorship study, though it is still likely a lower bound, owing to methodological and protocol limitations.

The analysis revealed a misconfigured blocking rule causing significant overblocking, where a major ISP blocked an entire gTLD (`.yokohama`). Blocking of domains across ISPs extended aggressively to services and platforms in categories including business, hosting, research, and communication. Additionally, a state-owned PSU ISP's consumer blocklist is hypothesized by the author to include domains supposed to be blocked only within government offices.

The scale of this study allowed for the production of evidence of significant overblocking which would otherwise not be captured. This is further emphasized when considering that only 9,363 (21.73%) blocked domains had a rank in the Tranco list. DNS filtering continues to remain a popular censorship technique for both small and large Indian ISPs. This will likely remain the case, unless there are major changes in the state's censorship policies.

Additional discussion

According to a 2024 report published by the Internet Watch Foundation (IWF), `.de` was the most abused TLD and the preferred “brand” for invite-based child abuse pyramid (ICAP) sites. The study’s findings correlate this. According to the IWF report, `.ru` was the second-most abused TLD for ICAP sites, though this study lacks coverage for the `.ru` TLD as an acknowledged limitation of the Active Domains list.

The unobscured list of domains classified as ICAP sites was supplied to the cyber tipline operated by the U.S. National Center for Missing and Exploited Children, as well as the National Cyber Crime Reporting Portal of the Indian Cyber Crime Coordination Centre.

No discretion was exercised over what domains to test, because publicly-available sources were used. Instances of illegal material being reported to relevant authorities was on a best-effort basis.

Recommendations for the internet freedom community

Certain jurisdictions regulate VPN and cloud infrastructure providers, but not the use of general network utility software, which could be designed to enable censorship circumvention without relying on external networks.

In the Indian context, VPN operators that make their services available to Indian residents are required to collect know-your-customer (KYC) data, and also store this information alongside usage logs for a period of five or more years, which means that censorship circumvention cannot rely on VPNs alone.

Tool developers and members of the internet freedom community should consider developing and promoting network utility tools that enable censorship circumvention without anonymizing traffic or relying on external network infrastructure.

Acknowledgements

This research was supported as part of the Information Controls Research Program funded by Open Technology Fund. The Internet Governance Project at the School of Public Policy at the Georgia Institute of Technology was the host organization.

The author acknowledges the technical feedback and guidance provided by Professor Paul Pearce, formerly at the School of Computer Science at the Georgia Institute of Technology, as well as the feedback and support of Jyoti Panday and Professor Milton Mueller.

The author is grateful for the support of the larger network measurement and censorship research communities, and also acknowledges the support of Wei Fan, Kiran Jonnalagadda, Nemo, Srinivas Kodali, Aditi Shah, and Tanveer Hasan.

Data and code availability

All collected measurements and resources are available at dnsblocks.in. The public blocklist release has been modified to obscure all sites classified as ICAP.

Tools:

- blockbust (wrapper around ZDNS with censorship detection utilities)
- domcat (UI for classifying domain categories)

Data:

- Raw DNS measurements (1.76 billion queries)
- Compiled blocklist, enriched with categories and Tranco ranks

Resources:

- Interactive blocklist explorer (available on the project website)

References

- APNIC Labs. n.d. “DNSSEC Validation Statistics.” https://stats.labs.apnic.net/dnssec.
- Ashiq, Peerzada. August 21, 2023. “Srinagar-based news portal The Kashmir Walla’s website in India blocked.” The Hindu. https://www.thehindu.com/news/national/website-social-media-handles-blocked-in-india-says-srinagar-based-news-portal-the-kashmir-walla/article67216978.ece.
- CERT-IN. April 28, 2022. “Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet.” Ministry of Electronics and Information Technology, Government of India. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.
- Citizen Lab and Others. 2014. “URL testing lists intended for discovering website censorship.” GitHub repository. https://github.com/citizenlab/test-lists.
- Domains Project. n.d. “Active Domains Dataset.” Accessed March 2025. https://domainsproject.org/.
- Durumeric, Zakir, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex Halderman. 2015. “A Search Engine Backed by Internet-Wide Scanning.” In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS ‘15). https://doi.org/10.1145/2810103.2813703. Platform available at https://search.censys.io/.
- Ganesan, Aarathi. November 15, 2023. “VideoLAN’s Website Is Up and Running Again: Here’s What We Know About the Unblocking.” Medianama. https://www.medianama.com/2022/11/223-videolan-vlc-website-unblocked-india-meity/.
- Gosain, Devashish, Anshika Agarwal, Sahil Shekhawat, H. B. Acharya, and Sambuddho Chakravarty. 2018. “Mending Wall: On the Implementation of Censorship in India.” In Security and Privacy in Communication Networks (SecureComm 2017). https://doi.org/10.1007/978-3-319-78813-5_21.
- Hoang, Nguyen Phong, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2021. “How Great is the Great Firewall? Measuring China’s DNS Censorship.” In the 30th USENIX Security Symposium (USENIX Security 21). https://www.usenix.org/system/files/sec21-hoang.pdf.
- ICANN. n.d. “Centralized Zone Data Service (CZDS).” Internet Corporation for Assigned Names and Numbers. https://czds.icann.org/.
- Internet Watch Foundation. April 23, 2024. “German .de domain ‘ruthlessly’ targeted by criminal gangs profiting from the sale of child sexual abuse images and videos.” https://www.iwf.org.uk/news-media/news/german-de-domain-ruthlessly-targeted-by-criminal-gangs-profiting-from-the-sale-of-child-sexual-abuse-images-and-videos/.

- Izhikevich, Liz, Gautam Akiwate, Phillip Doerfler, Liam Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. “ZDNS: A Fast DNS Toolkit for Internet Measurement.” In Proceedings of the 22nd ACM Internet Measurement Conference (IMC ’22). https://doi.org/10.1145/3517745.3561434. Software available at https://github.com/zmap/zdns.
- Katira, Divyank, Gurshabad Grover, Kushagra Singh, and Varun Bansal. 2023. “CensorWatch: On the Implementation of Online Censorship in India.” In Free and Open Communications on the Internet (FOCI ’23). https://www.petsymposium.org/foci/2023/foci-2023-0006.pdf.
- Kurkowski, John. n.d. “tldextract: Accurately separates a URL’s subdomain, domain, and public suffix, using the Public Suffix List (PSL).” Python library. GitHub repository. https://github.com/john-kurkowski/tldextract.
- lanrat. n.d. “czds: golang API and tools to interact with czds.icann.org.” GitHub repository. https://github.com/lanrat/czds.
- Le Pochat, Victor, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. “Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation.” In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://tranco-list.eu/.
- Ministry of Electronics and Information Technology, Government of India. June 29, 2020. “Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.” Press Information Bureau. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1635206&reg=3&lang=2.
- Pahwa, Nikhil. May 11, 2012. “DailyMotion Blocked In India On RCOM; Airtel & RCOM Block Bookmarking Site Xmarks.” Medianama. https://www.medianama.com/2012/05/223-dailymotion-blocked-in-india-on-rcom-airtel-rcom-block-bookmarking-site-xmarks/.
- Press Trust of India. November 24, 2023. “Follow orders if you want to do biz in India: HC to domain name registrars.” Business Standard. https://www.business-standard.com/india-news/follow-orders-if-you-want-to-do-biz-in-india-hc-to-domain-name-registrars-123112400818_1.html.
- Rathee, Kiran. June 10, 2025. “DoT Urges State Governments to Use BSNL and MTNL for Enhanced Data Security.” The Economic Times. https://economictimes.indiatimes.com/industry/telecom/telecom-news/dot-urges-state-governments-to-use-bsnl-and-mtnl-for-enhanced-data-security/articleshow/121736892.cms.
- Shodan. n.d. “Shodan: The Search Engine for Internet-Connected Devices.” https://www.shodan.io/.
- Singh, Kushagra, Gurshabad Grover, and Varun Bansal. 2020. “How India Censors the Web.” In Proceedings of the 12th ACM Conference on Web Science (WebSci ’20). https://doi.org/10.1145/3394231.3397891.
- Software Freedom Law Centre (SFLC), India. 2023. “FINDING 404: A Report on Website Blocking in India.” https://sflc.in/finding-404-report-website-blocking-india/.
- Srikanth, Kaustabh. January 6, 2015. “Observations on Recent India Censorship.” Security in a Box. https://securityinabox.org/en/blog/observations-recent-india-censorship/.
- SURBL BV. n.d. “Most Abused TLDs.” SURBL - Spam URI Realtime Block List. https://www.surbl.org/tld.
- Yadav, Tarun Kumar, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. 2018. “Where The Light Gets In: Analyzing Web Censorship Mechanisms in India.” In Proceedings of the Internet Measurement Conference (IMC ’18). https://doi.org/10.1145/3278532.3278555.

Appendix

A modified version of Citizen Lab's test list taxonomy. Changes are highlighted in bold.

Category	Code	Description
Alcohol & drugs	ALDR	Sites devoted to the use, paraphernalia, and sale of drugs and alcohol irrespective of the local legality.
Religion	REL	Sites devoted to discussion of religious issues, both supportive and critical, as well as discussion of minority religious groups.
Pornography	PORN	Hard-core and soft-core pornography.
Provocative attire	PROV	Websites which show provocative attire and portray women in a sexual manner, wearing minimal clothing.
Political criticism	POLR	Content that offers critical political viewpoints (includes critical authors and bloggers, oppositional political organizations, and pro-democracy and anti-corruption content).
Human rights issues	HUMR	Sites dedicated to discussing human rights issues in various forms. Includes women's rights and rights of minority ethnic groups.

Environment	ENV	Pollution, international environmental treaties, deforestation, environmental justice, disasters, etc.
Terrorism and militants	MILX	Sites promoting terrorism, violent militant or separatist movements. **Organizations officially banned by the Government of India are included in this list.**
Hate speech	HATE	Content that disparages particular groups or persons based on race, sex, sexuality, or other characteristics.
News media	NEWS	This category includes major news outlets (BBC, CNN, etc.) as well as regional news outlets and independent media.
Sex education	XED	Includes contraception, abstinence, STDs, healthy sexuality, teen pregnancy, rape prevention, abortion, sexual rights, and sexual health services.
Public health	PUBH	HIV, SARS, bird flu, centers for disease control, World Health Organization, etc.
Gambling	GMB	Online gambling sites (includes casino games and sports betting).
Anonymization and circumvention tools	ANON	Sites that provide tools used for anonymization, circumvention, proxy-services and encryption.
Online dating	DATE	Online dating services which can be used to meet people, post profiles, chat, etc.
Social networking	GRP	Social networking tools and platforms.
LGBT	LGBT	A range of gay-lesbian-bisexual-transgender, and queer issues (excluding pornography).

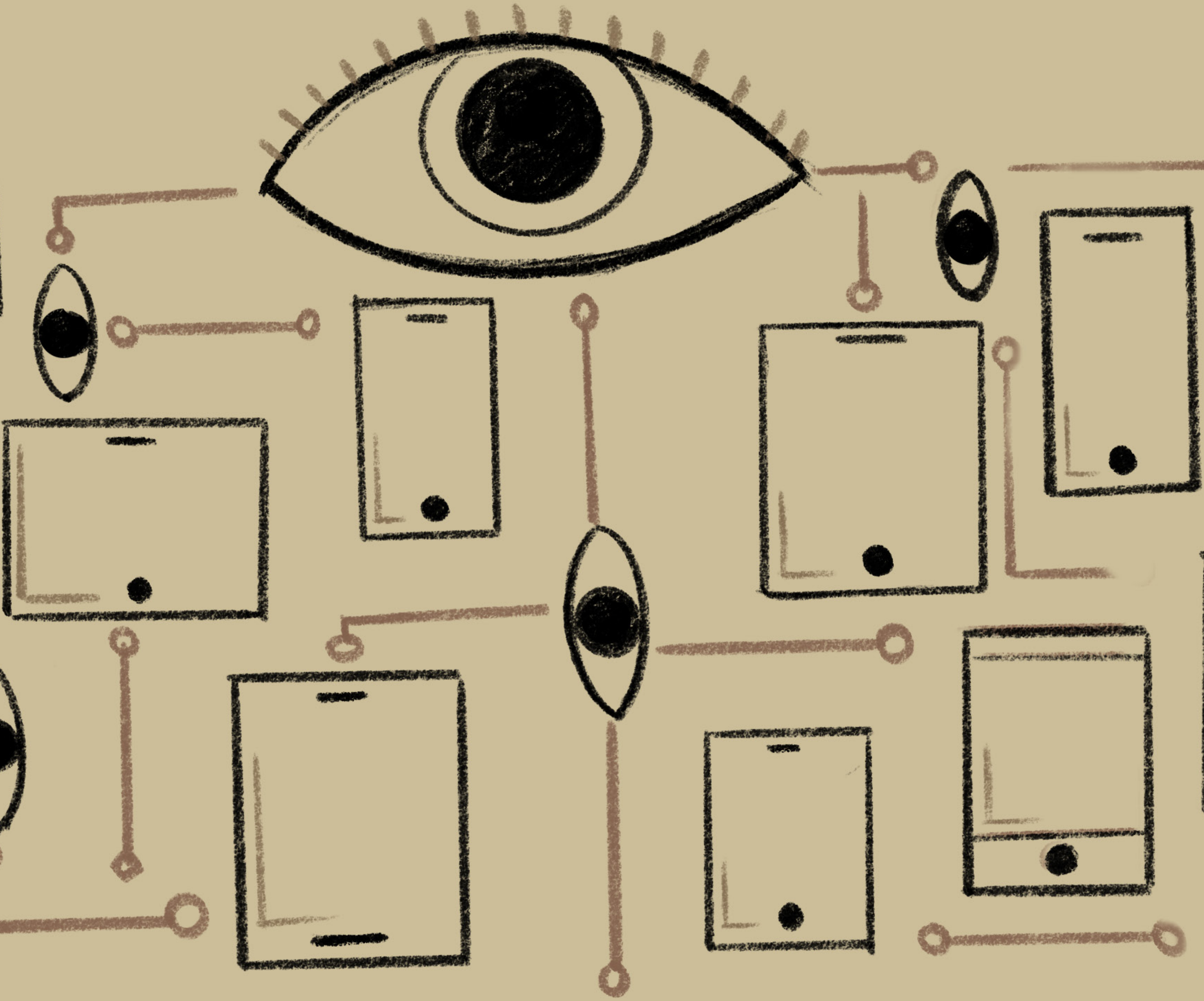
File sharing	FILE	Sites and tools used to share files, including cloud-based file storage, torrents and P2P file-sharing tools.
Hacking tools	HACK	Sites dedicated to computer security, including news and tools. Includes malicious and non-malicious content.
Communication tools	COMT	Sites and tools for individual and group communications, including webmail, VoIP, instant messaging, chat, and mobile messaging applications.
Media sharing	MMED	Video, audio, or photo sharing platforms.
Hosting and blogging platforms	HOST	Web hosting services, blogging, and other online publishing platforms.
Search engines	SRCH	Search engines and portals.
Gaming	GAME	Online games and gaming platforms, excluding gambling sites.
Culture	CULTR	Content relating to entertainment, history, literature, music, film, books, satire, and humor.
Economics	ECON	General economic development and poverty related topics, agencies, and funding opportunities.
Government	GOVT	Government-run websites, including military sites.
E-commerce	COMM	Websites of commercial services and products.
Control content	CTRL	Benign or innocuous content used as a control.

Intergovernmental organizations	IGO	Websites of intergovernmental organizations such as the United Nations.
Miscellaneous content	MISC	Sites that don't fit in any category
Malicious content	**MAL**	**Websites designed to phish, defraud, or otherwise harm users, including C2 domains and websites used in malware campaigns. Enriched with sites found in public security lists, e.g., github.com/maltrail/trails/static (as of 22 Sep, 2025). There may be an overlap with websites in the IPTM category.**
IP/trademark violations	**IPTM**	**Intellectual property violations, trademark, and copyright disputes, including brand impersonation sites. There may be an overlap with websites in the MAL category.**
Cryptocurrency	**COIN**	**Cryptocurrency exchange websites and related cryptocurrency trading platforms.**
Education	**EDU**	**Educational websites and platforms, including academic resources and educational institutions.**
Movies & TV	**MOV**	**Piracy websites specifically dedicated to movies and TV shows, including streaming and download sites for video content.**
Music & audio	**MUS**	**Piracy websites explicitly dedicated to music and audio files.**
Visa & immigration	**VISA**	**Visa application and immigration-related websites (may be official government sites, unofficial service providers, or scam websites).**

Business	BIZ	Websites that appear to be related to commercial businesses and corporate entities.
Text sharing	PASTE	Text sharing websites and paste services used for sharing code snippets, documents, and other text-based content.
Live streaming piracy	LIVE	Piracy websites providing livestreams of pay-per-view events such as football, cricket, MMA, and other sports or entertainment content.
Escort services	ESC	Websites advertising escort services.
Invite-based child abuse pyramid	ICAP	Child abuse material. Domains in this category have been reported to law enforcement and obscured in the data release.
Uncategorized	UNCAT	Uncategorized domains, distinct from the MISC category. The compiled blocklist includes generic uncategorized domains as well as Numeric Domain Names (NDNs), Internationalized Domain Names (IDNs), and domains with the .yokohama TLD.

OPEN TECHNOLOGY FUND

School of Public Policy
Internet Governance Project



Project website available at dnsblocks.in

Report prepared in March 2026. Copy edited by **Ameya Nagarajan** and **Ashley Lulling.**

Layout design by **Meher Rajpal.** Back cover illustration by **Rajat Kumar.**

Terminal Grotesque by **Raphaël Bastide**, with the contribution of **Jérémy Landes**.

Steps Mono by **Jean-Baptiste Morizot**, **Raphaël Bastide**. Distributed by velvetyne.fr.

Front cover is a remixed version of the illustration “Poisoned At The Source” by **Art Young.**