Review of

CensorWatch: On Implementation of Online Censorship in India

By Divyank Katira, Gurshabad Grover, Kushagra Singh, Varun Bansal

What is the problem?

The Government of India has the authority to order internet service providers (ISPs) to block access to certain websites and services through law orders, which are confidential, making it difficult for researchers or citizens to ascertain what websites are supposed to be blocked in India.

Summary

Indian law does not mandate ISPs to follow any specific technical method of blocking websites or URLs which results in inconsistencies in how ISPs conduct censorship, and find we find concrete evidence that ISPs in India are blocking different websites and engaging in arbitrary blocking, in violation of Indian law

Key Insights

Got insight about decentralised and centralised forms of **information controls.** Also learnt on the different levels of information control like DNS-, HTTP-, and SNI forms of censorship and projects that defend against like CitizenLab, OONI, censored planet.

Strengths

They used Largest set of potentially blocked websites, 10,372 unique hostnames.

Indian law does not mandate ISPs to follow any specific technical method of blocking websites or URLs, so they had to measure censorship on various levels, HTTP, DNS, SNI, and they explained their techniques well.

With 66 ISPs, any study must be run from several networks and locations to paint an accurate picture of online censorship in India, they collected and analysed measurements from 71 ASes and 25 states in the country.

They contextualised the blocking of specific websites with relevant legal orders and provide specific evidence of ISPs being non-compliant with legal orders, and arbitrarily blocking websites and services without a legal basis.

Limitations/Weaknesses

No testing for IP-based blocking or conditional TLS/HTTP filtering based on IP addresses. Only hostname-level analysis, no specific webpage blocking analysis.

SNI test doesn't capture potential censorship using ServerHello information in TLS connections.

Difficulty distinguishing between NXDomain DNS errors and generic DNS errors, hindering identification of censorship instances.

Summary of Key Results

The study found that HTTP-based blocking is the most popular censorship technique among Indian ISPs, observed in 64 out of 71 ASes. SNI-based blocking is used by 16 ASes, mainly by Bharti Airtel and Reliance Jio. DNS-based blocking is employed by 10 ASes, including Atria Convergence Technologies and BSNL. ISPs in India are blocking different websites despite receiving the same legal orders, indicating arbitrary censorship. Additionally, some ISPs block websites without legal justification, violating citizens' rights and net neutrality regulations.

Open Questions?

> Will the government and ISPs pay attention to policy and practical recommendations made in this paper and bring transparency and accountability to the state of censorship in India?