How India Censors the Web

Kushagra Singh∗
Centre for Internet and Society
kushagra17456@iiitd.ac.in

Gurshabad Grover∗
Centre for Internet and Society
gurshabad@cis-india.org

Varun Bansal
Centre for Internet and Society
varun13168@iiitd.ac.in

ABSTRACT
One of the primary ways in which India engages in online censorship is by ordering Internet Service Providers (ISPs) operating in its jurisdiction to block access to certain websites for its users. This paper reports the different techniques Indian ISPs are using to censor websites, and investigates whether website blocklists are consistent across ISPs. We propose a suite of tests that prove more robust than previous work in detecting DNS and HTTP based censorship. Our tests also discern the use of SNI inspection for blocking websites, which is previously undocumented in the Indian context. Using information from court orders, user reports, and public and leaked government orders, we compile the largest known list of potentially blocked websites in India. We pass this list to our tests and run them from connections of six different ISPs, which together serve more than 98% of Internet users in India. Our findings not only confirm that ISPs are using different techniques to block websites, but also demonstrate that different ISPs are not blocking the same websites.

1 INTRODUCTION
Nation states around the world engage in web censorship using a variety of legal and technical methods [10, 34, 44, 47]. India is no different in this regard: the Government of India can legally order internet service providers (ISPs) operating in its jurisdiction to block access to certain websites for its users. This makes the situation different from jurisdictions like Iran and China, where internet censorship is largely centralised [10, 13]. Legal provisions in India, namely Section 69A and Section 79 of the Information Technology (IT) Act, allow the Central Government and the various courts in the country to issue website-blocking orders that ISPs are legally bound to comply with [1, 2]. The implementation of these provisions create various uncertainties in how internet users experience web censorship:

First, the regulations do not mandate ISPs to use specific filtering mechanisms. Thus, ISPs are at liberty to employ various technical methods [47].

Second, website-blocking orders, especially those issued by the Government, are rarely available in the public domain. ISPs are, in fact, mandated by regulations to maintain confidentiality of certain website-blocking orders issued by the Government [3]. Various attempts by researchers and advocacy organisations to obtain the complete list of blocked websites have failed [4, 24].

Third, the whimsy of ISPs and the Government aggravates these problems. Despite strict net neutrality regulations in India that prohibit ISPs from arbitrarily restricting access to websites [35], some ISPs may be doing so nonetheless [21]. Reports also suggest that the Government has issued blocking orders and then rescinded them on the same day [40].

∗Both authors contributed equally to the paper

These concerns motivated us to study web censorship in India in detail. In particular, we seek to answer two questions pertaining to how internet users in India experience web censorship: (i) what are the technical methods of censorship used by ISPs in India? (ii) are all ISPs blocking the same websites? We contribute to research in documenting web censorship in India in three distinct ways:

Coverage of censorship mechanisms. Previous work has documented the use of DNS and HTTP based censorship techniques by Indian ISPs [47]. We include tests to determine whether ISPs are blocking websites based on the Server Name Indication, an extension in Transport Layer Security sessions. We find that Jio (an ISP serving 49.7% of internet users in India [36]) employs this technique. Additionally, we identify certain ISPs employing multiple censorship schemes, a fact previously undocumented in India.

Inconsistencies in websites being blocked. Although previous work records some inconsistencies in website blocklists across ISPs [47], they use a relatively smaller corpus of potentially blocked websites (1200). We curate the largest-known list of potentially blocked websites in India (4379), which has allowed us to draw extensive conclusions about how experiences of web censorship vary across ISPs. We also report cases of an ISP blocking websites that are not blocked by any other ISPs.

Accuracy of censorship detection techniques. Yadav et al. [47] point out some drawbacks of relying on OONI [19] for measuring internet censorship in India, and propose new methods of detecting DNS and HTTP based censorship. However, we find that their methodology to detect DNS censorship makes untested assumptions which we highlight and work around in our paper. Additionally, their HTTP censorship detection technique relies heavily on manual inspection, making a study at our scale untenable. We propose a novel HTTP censorship detection algorithm that requires no manual inspection, and is more accurate (in terms of F1 score) than previous automated methods.

2 RELATED WORK
There have been a fair number of previous studies which explore censorship mechanisms in different countries such as China [13, 31, 37, 46], Pakistan [7, 29, 34], Syria [12], Italy [7], Iran [10], and Korea [7]. Additionally, web censorship monitoring tools such as CensMon [42], and OONI [19] have allowed a similar analysis on a global scale. Such works highlight that countries across the world adopt a melange of techniques to censor the web.

Amongst the most prevalent is DNS based blocking, where the network responds to DNS queries for websites it wishes to block with either (i) DNS errors [30, 34, 38] or (ii) incorrect IP addresses [9, 10, 32, 44, 47]. Another popular technique employed by networks to filter websites is examining HTTP traffic and looking for (i) HTTP headers for blacklisted hostnames, or (ii) the HTTP request and/or response bodies for certain keywords [10, 15, 29, 34, 37, 42, 46].
Upon detecting such requests, censors have been found to either explicitly serve censorship notices [10, 34], close established HTTP connections [37], or both [47]. Some instances of filtering traffic by inspecting TCP/IP packets for destination blacklisted IP addresses have also been reported in Syria [12], Italy [7], and China [13]. There is also recent evidence that China is inspecting and filtering HTTPS web traffic based on the Server Name Indication present in the TLS handshake [13], but previous work has reported that no Indian ISP uses this technique [47].

In the Indian context, there has been an initial attempt to understand the censorship mechanisms employed by Indian ISPs [23, 47]. However, as we find, these studies have not uncovered the full extent of web censorship in India in terms of both technical mechanisms and scale.

3 DATA CURATION

We compile a list of potentially blocked websites from three types of sources:

**Government orders.** A website/URL blocking order may come from the Government of India [1, 2]. These orders are usually not in the public domain. For orders issued under section 69A of the IT Act, a confidentiality clause prevents any party from disclosing its contents [3]. We collect published and leaked Government orders, which contribute 890 URLs to our corpus.

**Court orders.** The various courts in India also have the power to issue website blocking orders [2]. Not all such orders are available in the public domain [27]. However, the Government and BSNL (a public company operating as an ISP) have provided portions of this list when under pressure to respond to Right to Information (RTI) requests. [4, 20]. Court orders contribute 9367 URLs to our list.

**User reports.** The Internet Freedom Foundation collects and publishes reports from internet users who notice blocked websites¹. These contribute an additional 62 URLs to our list.

Collecting data from these sources led to a total of 9673 unique URLs. Given that most of these URLs are sourced from recent court orders, there is a high possibility of them being currently blocked. The scope of our analysis is restricted to website-level (rather than webpage-level) blocking, and so we extract unique domain names from this list, resulting in 5798 websites. To limit ourselves to active websites, we exclude all websites for which we could not resolve via Tor circuits. We end up with a total of 4379 websites, which to the best of our knowledge, is the largest known corpus of potentially blocked websites in India.

4 METHODOLOGY

We propose the presence of different censorship techniques in six major Indian ISPs. These include Reliance Jio Infocomm (Jio), Bharti Airtel (Airtel), Vodafone Idea (Vodafone), Bharat Sanchar Nigam Ltd. (BSNL), Atria Convergence Technologies (ACT), and Mahanagar Telephone Nigam Ltd. (MTNL). The Telecom Regulatory Authority of India reveals that as of October 2019, these six ISPs together serve 657.46 million (98.82%) internet subscribers in India.

4.1 DNS censorship

Domain Name System (DNS) resolution involves translating a hostname to its corresponding IP address(es), and is usually the first step in accessing a website. Traditional DNS resolution is prone to poisoning and injection attacks [11]. There are secure resolution protocols such as DNSSEC [41], DNS over HTTP (DoH) [25], and DNS over TLS (DoT) [26] that mitigate these attacks; however, they are not widely deployed [14, 16].

**DNS Poisoning.** By default, DNS queries are sent to a resolver configured by the ISP. Thus, ISPs can return an incorrect IP address or nothing at all in response to clients’ DNS queries for websites they wish to block [10, 44, 48].

**DNS Injection.** ISPs can intercept DNS queries for websites they wish to block and inject incorrect IP addresses in the responses [9, 32, 38].

We term an ISP’s use of DNS poisoning or DNS injection attacks to block websites as DNS censorship.

4.1.1 Existing techniques. Detecting DNS censorship has previously been done by comparing responses from the test resolver with responses from trusted resolvers [19, 22]. However, this can lead to an over-reporting in censorship as these trusted resolvers can respond with a different IP address for legitimate reasons (such as load balancing) [8]. Lowe et al. circumvent this problem by selecting 5 censorship-free control resolvers and only investigating domain names for which all resolvers returned the same IP address; however, this results in a decrease in the size of the test list [31].

Another technique is to rely on the autonomous system (AS) number² to which the returned IP address belongs. Kührer et al. [30] consider a DNS response legitimate if the IP addresses returned via the trusted and tested resolvers belong to the same AS. This approach fails to take into account that a domain name can resolve to IP addresses belonging to different ASes. Yadav et al. deem a DNS response censored if the returned IP address belongs to the same AS as the client’s IP address [47]. This approach rides on two unsubstantiated assumptions: (i) that the incorrect IP address returned by the ISP always belongs to the same AS as the client’s, and (ii) the given website is not hosted within the same AS. Our proposed technique works around all these flaws.

4.1.2 Proposed technique. We begin by creating a set of IP addresses $IP_{d,C}$ for each domain name $d$ in our list by combining the responses obtained by resolving it via 5 censorship-free control networks (collectively termed $C$): (i) Tor circuits with exit nodes in US, CA and AU; and (ii) DoH servers run by Cloudflare and Google. In a test network, we attempt to resolve each domain name in our list using the ISP-assigned resolver. If the resulting IP address is present in $IP_{d,C}$, we conclude that the ISP is not using DNS censorship to block that website. Otherwise, similar to [30, 47], we flag the domain name censored if (i) the resolver responds with an error (for eg. NXDOMAIN), or (ii) the resolver responds with a bogon IP³. We further investigate the list of domain names $D'$, for which the ISP-configured resolver returns an IP address not found in $IP_{d,C}$. For these domain names, the test network is returning either (i) a legitimate IP address not captured via the control networks, or

---

¹[https://bit.ly/ifuserreport](https://bit.ly/ifuserreport)

²[https://www.apnic.net/get-ip/faqs/asn/](https://www.apnic.net/get-ip/faqs/asn/)

³[https://ipinfo.io/bogon](https://ipinfo.io/bogon)
(ii) an incorrect IP address. We term the second possibility as DNS tampering. As [10, 47] report, ISPs implementing DNS tampering respond with the same incorrect IP address to DNS queries for websites it wishes to block. We try to identify such behaviour by an ISP by looking at all IP addresses being returned by it for domain names in $D'$. For each network $n$, we construct $IP_n$, the list of IP addresses received by resolving domain names in $D'$ via that network. Next we calculate $MRF_n$, the relative frequency of the most frequent IP address in $IP_n$. By comparing $MRF$ values of the test and control networks, we are able to discern if the test network responds with an abnormally recurring IP address. This would be characteristic of an ISP that is censoring websites by returning an incorrect IP address, i.e. employing DNS tampering\(^3\). In ISPs where we detect DNS tampering, we mark domain names for which the DNS response was the most frequent IP address as censored.

**Algorithm 1: DNS Tampering Detection**

**Input:** Test Network $T$, List of Domain Names $D$

**Result:** Determines DNS tampering

1. $C \leftarrow \{C_1, C_2, \ldots, C_k\}$ // control networks (Tor, DoH)
2. for $d \in D$ do
   3. for $c \in C$ do
      4. $IP_{d,c} \leftarrow$ DNS response for $d$ collected via $c$
      5. $\{IP_{d,c}\} \leftarrow |IP_{d,c}| \subset C$
      6. $IP_{d,t} \leftarrow$ DNS response for $d$ collected via test network
     7. $D' \leftarrow \{d|d \in D \land IP_{d,t} \notin IP_{d,c}\}$ // domain names for which test response did not match any of control responses
3. for $c \in C$ do
   4. for $d \in D'$ do
      5. $IP_{d,c} \leftarrow$ DNS response for $d$ collected via $c$
      6. $IP_c \leftarrow \{IP_{d,c}|d \in D'\}$
5. for $ip \in IP_c$ do
   6. $RF_{ip,c} \leftarrow$ Relative frequency of $ip$ in $IP_c$
   7. $MRF_c \leftarrow \max\{RF_{ip,c}|ip \in IP_c\}$
   8. $\mu_{MRF_c} \leftarrow$ mean of $MRF_c \forall c \in C$
   9. $\sigma_{MRF_c} \leftarrow$ standard deviation of $MRF_c \forall c \in C$
10. for $d \in D'$ do
    11. $IP_{d,t} \leftarrow$ DNS response for $d$ in test network
    12. $IP_t \leftarrow \{IP_{d,t}|d \in D'\}$
13. for $ip \in IP_t$ do
   14. $RF_{ip,t} \leftarrow$ Relative frequency of $ip$ in $IP_t$
   15. $MRF_t \leftarrow \max\{RF_{ip,t}|ip \in IP_t\}$
   16. if $MRF_t - \mu_{MRF_t} > 3 \ast \sigma_{MRF_t}$ then
      17. return DNS Tampering present
   18. else
      19. return DNS Tampering not present

4.2 TCP/IP Blocking

ISP can block access to websites by preventing clients from connecting to the specific IP addresses the website is hosted on \([7,12,13,42]\). Additionally, the ISP may inspect TCP packet headers for the destination port number if it wishes to block certain types of traffic for that IP address. However, this censorship technique can result in over-blocking due to the popularity of virtual hosting, which allows multiple websites to be hosted on the same IP address \([17]\). These pitfalls are a plausible explanation for why ISPs in Korea \([7]\), Iran \([10]\) and Pakistan \([7,34]\) do not use this technique. Yadav et al also conclude the same for Indian ISPs\([47]\); however, it is unclear how they determine what IP addresses to probe to detect such censorship.

4.2.1 Proposed technique

We first obtain legitimate IP addresses for websites in our test list as discussed in section 4.1.2. This precludes any DNS censorship by ISPs from interfering with our test. Building on \([42,47]\), we perform a two-step test. First, we ping\(^5\) the IP address to verify whether it is reachable through the test network. A response implies that the ISP is not filtering traffic based on the destination IP address. For such IP addresses, we then attempt to establish a TCP connection on ports 80 (used for HTTP traffic) and 443 (used for HTTPS traffic). A successful TCP 3-way handshake with a given IP address and port would imply the absence of TCP-based blocking. A failure in either step, however, can be attributed to network congestion, host unavailability or, of course, censorship by the ISP. To establish that connection failures are indeed due to censorship, we run the same tests via Tor circuits with exit nodes in censorship-free countries (USA, CA, and AU). We rule out host unavailability and network congestion by reattempting failed connections five times with a delay of 100 seconds.

4.3 HTTP Filtering

Unencrypted HTTP traffic between a client and host can be intercepted and monitored. Previous studies have discovered different techniques adopted by censors for blocking HTTP access \([10,29,34,37,42]\). When a client attempts to access a website that the ISP seeks to block, the ISP sends back forged TCP or HTTP packets that seem to be originating from the host. These can include (i) a TCP packet with the RST (reset) bit set, forcing the client to kill the connection instantly \([37]\), (ii) an HTTP 2xx response\(^6\) containing a censorship notice \([34]\), (iii) an HTTP 3xx response\(^6\) redirecting the client to a URL serving a censorship notice \([34]\), or (iv) an HTTP 4xx/5xx response\(^6\) conveying an HTTP error to the client \([10]\).

4.3.1 Existing techniques

Due to the size of our corpus, we cannot rely on manual inspection as done by \([47]\). Existing automated techniques for detecting censored HTTP responses usually rely on making comparisons with uncensored responses, collected either via control servers set up in censorship-free countries \([7,42]\), or via Tor circuits \([18,19,45,47]\). Due to the dynamic nature of content hosted on websites, comparing verbatim responses can be error-prone \([28]\). Moreover, the geographical location of a client can also introduce variations (such as the content language) in the received response. To mitigate these issues, prior research utilizes meta information derived from responses for comparison \([19,28,45]\).

\(^3\) We leverage the fact that most websites in our curated list have a high possibility of being blocked. See section 3

\(^5\) [HTTP response codes (RFC 7233)](https://tools.ietf.org/html/rfc7231#section-6.1)

\(^6\) [Linux ping](https://linux.die.net/man/8/ping)
Jones et al. propose methods for identifying HTML pages which contain a censorship notice [28]. They report that comparing a test response’s length and HTML DOM structure with that of an uncensored response can help identify such pages with a high accuracy. Similarly, other authors use response length in conjunction with different HTML similarity metrics for comparisons [7, 18, 19]. However, these approaches perform well only in instances where censors explicitly inject censorship notices, an assumption that generally doesn’t hold true: as discussed above, censors have been known to adopt tacit approaches such as responding with HTTP errors or redirections. In the absence of HTML responses, these methods depend solely on response lengths, which as [47] discover, can be ineffectual [47]. The OONI tool [19] does a more elaborate comparison, drawing conclusions by observing differences in status codes, headers, lengths, and HTML titles. However, even their approach culminates in false positives and false negatives [47].

Building upon these approaches, we propose a more robust automated technique for detecting censored responses (outlined in algorithm 2) and use it to probe Indian ISPs for HTTP censorship.

4.3.2 **Collecting HTTP responses.** We begin by resolving the IP address of each domain name in our list via trusted resolvers, as discussed in section 4.1.2. Since DNS resolution may return multiple IP addresses for the same domain name, we probe all resulting (domain name, IP address) pairs in our experiment.

For each (domain name, IP address) pair, we make HTTP GET requests to the IP address, with the host header set as the domain name. This is done via 5 control servers in censorship-free countries (US, CA, GB, NE, and AU), and via the test network. Unlike some studies [18, 19, 45, 47] we avoid using Tor circuits for collecting control responses, since some websites blacklist them and respond differently to HTTP requests originating from them. Additionally, instead of using just one control response [19, 28, 47], we consider multiple responses.

4.3.3 **Proposed technique.** After collecting the control and test responses, we follow the detection technique outlined in algorithm 2. First, we compare the HTTP status code of control responses with that of the test response. If these status codes do not match, we classify the test response as censored. However, the opposite need not necessarily imply the absence of censorship. In case the status codes are the same, we investigate further on a case by case basis as explained below.

- **2xx (Success):** We check for response length inconsistency and response body inconsistency.
- **3xx (Redirection):** We compare the domain name present in the redirect URLs.
- **4xx/5xx (Error):** We compare the session header keys.

The response length inconsistency and response body inconsistency used above is defined as follows

**Response length inconsistency.** Given control response lengths \(L_c_1, L_c_2, \ldots, L_c_n\) and a test response length \(L_t\), we call \(L_t\) inconsistent if \(|\mu_c - L_t| > 3\sigma_c\), where \(\mu_c\) is the mean, and \(\sigma_c\) the standard deviation of the control response lengths.

**Response body inconsistency.** For each control and test response, we generate term frequency (TF) vectors using HTML tags extracted from the response body. A test response body is called inconsistent if \(|\mu_t - \mu_c| > 3\sigma_{tc}\), where \(\mu_t\) and \(\mu_c\) are the mean cosine similarity between TF vectors of control responses, \(\mu_t\) the mean cosine similarity between TF vectors of test and control responses, and \(\sigma_{tc}\) the standard deviation of cosine similarity between TF vectors of control responses.

To verify the efficacy of our proposed technique, we manually inspect 500 responses from the six ISPs (a total of 3000 responses), and categorise them as censored or uncensored. We implement the previous techniques and compare their predictions on the annotated set to ours. As reported in table 1, our proposed technique detects both censored and uncensored responses with a higher f1-score than previous approaches.

**Algorithm 2: HTTP Censorship Detection**

**Input:** DOMAIN NAME dn, IP ADDRESS ip

**Result:** Determines HTTP censorship

1. control_res ← HTTP GET response for dn.ip in control networks;
2. test_res ← HTTP GET response for dn.ip in test network;
3. if connection reset while getting test_res then return censored;
4. if control_res.status_code ≠ test_res.status_code then return censored;
5. else if test_res.status_code = 2xx then return censored;
6. if test_res.length inconsistent OR test_res.body inconsistent then return censored;
7. else if test_res.status_code ≠ 3xx then return censored;
8. if mismatch in control_res, test_res redirect HOSTNAMEs then return censored;
9. else return uncensored;
10. else if mismatch in control_res, test_res redirect keys then return censored;
11. else return uncensored;

**Figure 1:** Performance of various HTTP censorship detection techniques. We report Precision, Recall and F1-score for Censored (C) and Uncensored (U) classes. Our proposed technique has a higher F1-score than the previous techniques.

### Table 1: Performance of various HTTP censorship detection techniques.

| Detection Technique | Precision | Recall | F1 score |
|---------------------|-----------|--------|----------|
|                      | C  | U  | C  | U  | C  | U  |
| Length difference [28, 47] | 0.65 | 0.73 | 0.77 | 0.59 | 0.70 | 0.66 |
| HTML similarity [28] | 0.45 | 0.44 | 0.62 | 0.28 | 0.52 | 0.34 |
| OONI [19] | 0.67 | 1.00 | 1.00 | 0.54 | 0.80 | 0.70 |
| Proposed | 0.71 | 0.98 | 0.99 | 0.63 | 0.83 | 0.77 |

**4.4 SNI Based Censorship**

The Server Name Indication (SNI) was designed as an extension to TLS to support the hosting of multiple HTTPS websites on the same IP address [6]. The SNI is an attribute included in the ClientHello message, where the client specifies the hostname it wishes to connect to. Since the SNI is in clear-text, censors can monitor this field for hostnames and block websites by preventing successful TLS connections [13, 33, 43, 49]. While such censorship has been
documented in China [13] and Korea [5], there has been no prior evidence to suggest that Indian ISPs are using this technique [47].

4.4.1 Proposed technique. For this test, we take advantage of a server configured to accept TLS connections even if it does not host the website specified in the SNI. For each potentially blocked website, we attempt to establish a TLS version 1.3 connection with that server’s IP address using the website’s hostname as the SNI. A successful connection would imply the absence of SNI-inspection based censorship in the test network. Using TLS version 1.3 ensures that only the IP address and servername are present in clear-text, since all subsequent communication after the ClientHello and ServerHello is encrypted [39]. This precludes the interference of any other censorship technique used by the ISP with our test.

5 RESULTS
We first report the different censorship techniques adopted by ISPs, and then compare the consistency of website blocklists across ISPs.

5.1 Censorship techniques
We notice stark differences in censorship mechanisms adopted by Indian ISPs, each using a range of techniques individually or in combination to censor websites (outlined in Table 2).

| ISP | DNS | TCP/IP | HTTP | SNI |
|-----|-----|--------|------|-----|
| ACT | ✓   | ✓      | ✓    | ✗   |
| Airtel | ✓   | ✗      | ✓    | ✓   |
| BSNL | ✓   | ✗      | ✗    | ✗   |
| Jio | ✗   | ✗      | ✓    | ✓   |
| MTNL | ✓   | ✗      | ✗    | ✗   |
| Vodafone | ✗   | ✗      | ✓    | ✓   |

Table 2: Censorship techniques employed by Indian ISPs

Interestingly, we notice different trends as compared to the previous study on Internet censorship in India [47]: (i) They report Airtel to be using only HTTP header inspection based censorship for blocking websites. We notice otherwise, with Airtel using DNS censorship in conjunction with the aforementioned technique. (ii) They report no instances of SNI-inspection based censorship in any ISP, whereas we observe Jio to be using it extensively for blocking (2951 websites). These new observations indicate an evolving nature of censorship mechanisms employed by Indian ISPs. Further, we notice that all ISPs using multiple censorship mechanisms are not blocking the same websites with each mechanism. For instance, ACT uses only DNS censorship for blocking 233 websites, only HTTP censorship for 1873 websites, and both to block 1615 websites. Such irregularities are illustrated in figure 1.

5.1.1 DNS. We observed DNS censorship in four ISPs: ACT, Airtel, BSNL, and MTNL. Airtel is unique in responding with NXDOMAIN errors to DNS queries for websites it blocks. We notice otherwise, with Airtel using DNS censorship in conjunction with the aforementioned technique. (ii) They report no instances of SNI-inspection based censorship in any ISP, whereas we observe Jio to be using it extensively for blocking (2951 websites). These new observations indicate an evolving nature of censorship mechanisms employed by Indian ISPs. Further, we notice that all ISPs using multiple censorship mechanisms are not blocking the same websites with each mechanism. For instance, ACT uses only DNS censorship for blocking 233 websites, only HTTP censorship for 1873 websites, and both to block 1615 websites. Such irregularities are illustrated in figure 1.

Figure 1: Censorship techniques used by (i) ACT, (ii) Airtel, and (iii) Jio for blocking websites. We notice the same ISP using multiple techniques for blocking different websites.

ISPs were using DNS tampering. For illustration, Figure 2 compares the frequency of IP addresses received for DNS queries for potentially-blocked websites in four networks: an ISP that uses DNS-based censorship (ACT), and three Tor circuits with exit nodes in censorship-free countries. Each of these three ISPs responded with a unique incorrect IP address. Using this fact, we conclude that there was no collateral censorship from DNS-based blocking by other ISPs.

5.1.2 TCP/IP. Given the immense collateral censorship caused by TCP/IP based methods of censorship, we were not surprised to find that, in line with [47], no ISP we investigated uses this technique.

5.1.3 HTTP. We observe HTTP-header based censorship in all the six ISPs we investigated, but find only ACT, Airtel, Jio, and Vodafone to be serving distinct censorship notices. Additionally, we notice Airtel to be closing connections and not serving any censorship notice for the majority of the websites it blocks. Using the unique signatures of these responses, we are able to identify collateral censorship in other ISPs stemming from these ISPs. For instance,
we find that all instances of HTTP censorship we detect in BSNL and MTNL are attributable to Airtel and ACT. There was also a small number of instances where we observed Vodafone’s censorship notices from tests run through Jio (2), and Airtel’s notices in tests run through Vodafone (2).

5.1.4 SNI Inspection. We observe SNI inspection based censorship only in one ISP, Jio. Since we did not observe SNI-based censorship in any another ISP, we rule out collateral censorship caused by Jio’s employment of this technique. Out of 3340 websites we found Jio to be censoring, we notice the use of SNI inspection for 2951 websites. The only previous study on censorship practices in India summarily dismissed its use by Indian ISPs, including Jio [47].

5.2 Website blocklists
If we observe a particular ISP blocking a website by any method, we mark it as censored by that ISP. We term this list of censored websites by a particular ISP as its website blocklist. Note that for an ISP’s blocklist, we only consider websites are censored by the ISP using its own mechanisms, i.e. we ignore collateral censorship which we highlighted in section 5.1).

From our list of 4379 potentially blocked websites that we tested, we find that 4033 appear in at least one ISP’s blocklist. We use this list of 4033 websites for further analysis to see whether website blocklists are consistent across ISPs.

Interestingly, we notice large inconsistencies in ISPs’ blocklists. For instance, we find that in terms of absolute numbers, ACT blocks the maximum number of websites (3721). Compared to ACT, Airtel blocks roughly half the number of websites (1892). Table 2 notes the size of each ISP’s blocklist. Perhaps most surprisingly, we find that only 1115 websites out of the 4033 (just 27.64%) are blocked by all six ISPs. Figure 3 illustrates the variation in different ISPs’ blocklists.

We also found that several websites (215) are being blocked by only a single ISP out of the six. For instance, ACT blocks 62 websites that are not blocked by another ISP. This calls into question whether blocking of these websites has any standing legal basis, and is potential evidence of the fact that ISPs are blocking websites arbitrarily.

| ACT  | Airtel | BSNL | Jio  | MTNL | Vodafone |
|------|--------|------|------|------|----------|
| 3721 | 1892   | 3033 | 3340 | 3182 | 2273     |

Table 3: Number of websites (out of 4033) blocked by ISPs

6 CONCLUSION
Our work presents the largest study of web censorship in India, both in terms of number of censorship mechanisms that we test for, and the corpus size of the potentially-blocked websites. In terms of censorship methods, our results confirm that ISPs in India are at liberty to use any technical filtering mechanism they wish: there was, in fact, no single mechanism common across ISPs. We also found a deep packet inspection technique, namely SNI inspection, already being employed by the largest ISP in India (Jio) to censor websites. Our work also records large inconsistencies in website blocklists across ISPs in India. Simply stated, we find conclusive proof that Internet users in India can have wildly different experiences of web censorship.

Figure 3: Heatmap illustrating the overlap of blocklists of different ISPs. For each pair of ISP blocklists $L_a$ and $L_b$, we calculate $\frac{|L_a \cap L_b|}{|L_a \cup L_b|}$.

Analysing inconsistencies in blocklists also makes it clear that ISPs in India are (i) not properly complying with website blocking (or subsequent unblocking orders), and/or (ii) arbitrarily blocking websites without the backing of a legal order. This has important legal ramifications: India’s net neutrality regulations, codified in the license agreements that ISPs enter with the Government of India[35], explicitly prohibit such behaviour.

Our work also points to how the choice of technical methods used by ISPs to censor websites can decrease transparency about state-ordered censorship in India. While some ISPs were serving censorship notices, other ISPs made no such effort. For instance, Airtel responded to DNS queries for websites it wishes to block with NXDOMAIN. Jio used SNI-inspection to block websites, a choice which makes it technically impossible for them to serve censorship notices. Thus, the selection of certain technical methods by ISPs exacerbate the concerns created by the opaque legal process that allows the Government to censor websites.

Web censorship is a curtailment of the right to freedom of expression guaranteed to all Indians. There is an urgent need to reevaluate the legal and technical mechanisms of web censorship in India to make sure the curtailment is transparent, and the actors accountable.

7 FUTURE WORK
Evolving censorship mechanisms adopted by the ISPs also imply that censorship-evasion techniques have to evolve in tandem. Future research can focus on developing tools that help Indian netizens evade website blocking. The whimsical attitude towards web censorship from both ISPs and the Government may also necessitate the development of a crowdsourced tool to monitor and measure such censorship from different vantage points in the country.
