Mind the IP Gap

On the IPv6 Transition and the Emergence of DNS Censorship Inconsistencies

Paper #XXX

Abstract

This is our abstract

1 Introduction

Internet censorship is a global problem that affects over half the world's population. Censors rely on sophisticated network middleboxes to inspect and block traffic. A core component of Internet censorship is DNS blocking, and prior work has extensively studied how DNS censorship occurs, both for specific countries [4, 19] and globally [12, 22, 33, 35]. These studies generally perform active measurements of DNS resolvers for large sets of domains, and identify forged censorship responses from legitimate ones.

Unfortunately, prior work has focused exclusively on the IPv4 Internet, in part because scanning the IPv6 Internet for open resolvers is difficult [28], owing to its impossible-to-enumerate 128-bit address space. In this paper, we perform the first comprehensive global measurement of DNS censorship on the IPv6 Internet. We leverage a recent network measurement technique that can discover dual-stack IPv6 open resolvers from their IPv4 counterpart [18], and use these IPv4-IPv6 resolver pairs to study DNS censorship globally. By sending DNS queries to both the IPv4 and IPv6 interfaces of the *same resolver*, we measure the difference in censorship on the IPv4 and IPv6 Internet.

IPv6 is becoming more widely deployed, with nearly 35% of current Internet traffic being served over native IPv6 connections [2]. However, IPv6 has fundamentally different performance characteristics [13], network security policies [11], and network topologies [10].

While it may seem that censors either do or don't support detecting and censoring IPv6 DNS, we find that there is a tremendous range of how well a censor blocks in IPv6 compared to IPv4. In particular, although nearly all of the countries we study have some support for IPv6 censorship, we find that most block less effectively in IPv6 compared to IPv4. For instance, we observe Thailand censors on average 80% fewer IPv6 DNS resources compared to IPv4 ones, despite a robust nation-wide censorship system [17].

Studying censorship in IPv6 can provide opportunities for circumvention tools. By identifying ways that censors miss or incorrectly implement blocking, we can offer these as techniques that tools can exploit. Moreover, because of the complex and heterogeneous censorship systems censors operate, many of these techniques would be costly for censors to prevent, requiring investing significant resources to close the IPv4/IPv6 gap in their networks. For this reason, we believe IPv6 can provide unique techniques for circumvention researchers and tool developers, that will be beneficial in the short term, and potentially robust in the longer term.

We find a significant global presence of IPv6 DNS censorship – comparable, but not identical to well documented IPv4 censorship efforts. Censors demonstrate a clear bias towards IPv4, censoring `A` queries in IPv4 at the highest rates, and a propensity for censoring native record types (`A` in IPv4, `AAAA` in IPv6). At the country level we break down differences by resolver and domain across resource record and interface type. We find that multiple countries – Thailand, Myanmar, Bangladesh, Pakistan, and Iran – present consistent discrepancies across resolvers or domains indicating centrally coordinated censorship, where IPv4 and IPv6 efforts are deployed or maintained independently but managed centrally. Other countries show inconsistent discrepancies in the ways that resolvers censor IPv4 and IPv6 with resolvers that can be loosely grouped by AS connection type (for the AS where the resolver is located) and the set of domains that each resolver censors. This evidence supports a decentralized model of censorship coordination or deployment in countries like Russia and China.

We also identify behavior indicative of censorship oversight that can be advantageous to censorship circumvention. For example Iran censors queries that rely on 6to4 bridges at significantly lower rates presumably due to the encapsulation of an IPv6 DNS request in an IPv4 packet marked as type IPv6 encapsulation.

Taken all together, this study provides a first look at IPv6 DNS censorship and the policy gaps that arise from the IPv6 transition. We provide the following contributions:

- We conduct the first large-scale measurement of IPv6 DNS censorship in over 100 IPv6-connected countries. We find that while most censors support IPv6 in some capacity, there are significant gaps in how well they censor IPv6.

- We provide methodological improvements on measuring DNS censorship that avoids relying on cumbersome IP comparisons (that are not robust to region-specific DNS nameservers). Our methods are easily reproducible, and can be used in future measurement studies

- We characterize the difference in censorship of both network type (IPv4 and IPv6), and resource type (`A` and `AAAA` record), and identify trends in several countries.
- Using our findings, we suggest several new avenues of future exploration for censorship circumvention researchers, and censorship measurements.

The remainder of this paper is layed out as follows. §2 provides background information in DNS censorship, and the relation of IPv6 to relevant DNS infrastructure. We outline our compiled methodology and ethical design considerations in §3 before presenting our findings on the global prevalence of IPv6 censorship in §4. We then dig into per country analysis based on Resource Record types in §5 and IP protocol version in §6. We select several case studies to highlight in §7 before covering related work in §8. Finally §9 provides discussion and contextualization of this work before concluding.

2 Background

Network based censorship is a common barrier to global internet access today. In some instances this manifests as corporate access control mechanisms deployed to protect internal networks and intellectual property. However, state actors have the ability to incorporate large scale network monitoring systems into national network infrastructure preventing access to information through either active interference or threat of retribution. There have been many studies on censorship techniques both globally [16, 30, 32, 33, 35, 37] and within individual countries [5, 17, 19, 29, 34, 43].

Internet infrastructure is evolving to accommodate global connectivity as well – IPv6 deployment provides routable addressing to an increasing portion of the internet as IPv4 allocations become scarce. Effective censorship strategies attempting to control or limit accessibility have to keep up. Censorship strategies are capable of reactive change as demonstrated by the impact that real world events like elections [5], social or political unrest [31, 36], and specifically crafted circumvention tools [7] have on blocking techniques and block-lists. Documenting contemporary censorship strategies through the transition from IPv4 to IPv6 can help to understand the the trajectory of network censorship efforts more broadly.

2.1 DNS Censorship Measurement

The Domain Name System (DNS) underpins the global internet by providing a mapping from human readable hostnames to routable IP addresses making domain name resolution the first step in almost all connection establishment flows. However, the widely deployed DNS system is implemented as a plaintext protocol allowing on-path eavesdroppers to inspect the hostnames as clients attempt to establish connections and in some cases inject falsified responses to interfere.

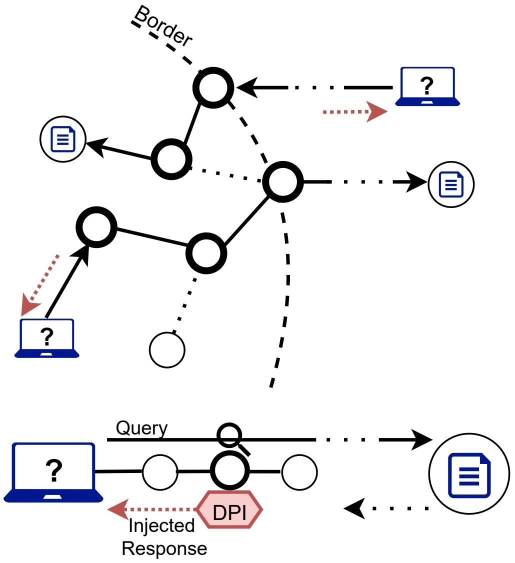

Figure 1: DNS censorship is carried out by on-path or in-path deep packet inspection (DPI) appliances that monitor for block-listed keywords or expressions in DNS queries and inject forged responses. The original request and subsequent response are not typically dropped by the adversary, but will arrive after the forged response rendering them useless. DPI appliances can be deployed in local infrastructure, regional ISPs, or national border gateways and inject the forged response toward the query source in either direction.

The Chinese traffic inspection system, called the Great Firewall (GFW), is documented injecting falsified DNS responses as early as 2002 [9]. This censorship has been shown to be a packet injection from an on-path adversary monitoring for hostnames in DNS queries that match regular expressions [19]. An on-path adversary operates on a copy of traffic transiting a specific link or gateway in a network. This contrasts with an in-path adversary which operates on traffic inline with the capability to drop or modify packets on the fly. These traffic inspection devices can be housed at or near border gateways [42] or distributed throughout regional ISPs [34] within censoring countries. Notably the GFW and other on-path DNS censorship appliances will inject responses in either direction (downstream into the country or upstream out out of the country) to the source of the query. This allows measurements of deployed censorship infrastructure to be launched from outside of the country in question as long as the query transits a monitored link.

Common strategies for measuring censorship via DNS injection involve routing DNS queries for block-listed hostnames across a censoring link in a controlled environment where the returned resource records can be independently validated. Two notable previous studies Satellite and Iris [33, 35] identify open DNS resolvers across the internet by scanning the entire IPv4 space on port 53. Satellite probes reliably available open resolvers from a set of distributed vantage points and detects incorrect or inconsistent response information. Iris develops a method for identifying active manipulation in contrast to misconfiguration by leveraging metrics such as consistency and independent verifiability. Iris compares records returned by open resolvers to records returned a set of trusted resolvers matching IP addresses, content hash, TLS certificate, and more. In order to identify open resolvers both Satellite and Iris rely on the zmap internet wide scanning tool [15] limiting themselves to the IPv4 address space.

2.2 IPv6 & DNS

The proportion of clients that support IPv6 is rapidly growing, especially in developing areas with newly deployed network infrastructure. According to the APNIC internet registry over a quarter of the users on the internet now route their traffic using IPv6 [20]. Similarly Google metrics indicate that over 50% of users access services using IPv6 in India, Saudi Arabia, Germany and several other countries [2]. As with many other critical internet protocols, DNS implements an IPv6 extension to maintain relative uniformity in connection establishment flows.

A vs AAAA. DNS `A` queries and records respectively request and provide resources to resolve hostnames into IPv4 addresses. `AAAA` queries and records resolve hostnames to IPv6 addresses.

IPv4 vs IPv6 Queries. The type of resource requested is indicated in the `query_type` portion of a DNS request and is not linked to the IP version that the DNS query is sent over - i.e. both `A` and `AAAA` can be resolved over IPv4 or IPv6. Some hostnames resolve exclusively to IPv4 or IPv6 i.e. only provide `A` or `AAAA` records respectively, as is the case for many legacy sites on the internet that only support IPv4.

A theoretically comprehensive DNS censorship strategy using response injection requires traffic monitoring infrastructure to analyze both IPv4 and IPv6 traffic and parse both `A` and `AAAA` queries accounting for hostnames that may not implement resource records of one type or the other. Such a strategy would only impede connections that use plaintext DNS (as outlined in the original specifications [27, 38]) - it would not effect more secure DNS protocols such as DoT, DoH, or censorship resistance strategies which are not covered in this work.

Discovering Dual-Stack Open Resolvers. Hendricks et al. describe in depth a method for discovering and validating DNS resolvers that expose both IPv4 and IPv6 interfaces [18]. They start with an initial set of IPv4 resolvers discovered using zmap. This set is then sent a query for a specially crafted domain containing a subdomain whose nameserver supports only IPv6. In an attempt to recursively resolve the domain the resolver will connect to the controlled nameserver using an IPv6 address if one is available. Subsequent queries are then used to identify configurations that forward or distribute queries indicating address pairs that are not truly dual-stack resolvers.

Our work combines these strategies to investigate the global prevalence of DNS injection in IPv6.

3 Dataset and Methodology

The analysis presented in the remainder of this paper is based on the results of 21.3M DNS `A` and `AAAA` resolution requests for 717 domains sent to 7,428 IPv4- and IPv6-capable resolvers located in a 106 countries. In this section, we explain our process for identifying resolver targets for our queries (§3.1), domains that are the subject of our queries (§3.2), and our process for identifying the occurrence of a censorship event from the results of each query (§3.3).

3.1 Selecting resolvers

Our work is aimed at characterizing the inconsistencies that exist in the handling of IPv4- and IPv6-related DNS queries — i.e., differences in the handling of `A` and `AAAA` query types over IPv4 and IPv6 connections. Therefore, we required that each resolver used for our measurements was IPv4- and IPv6-capable.

Identifying resolvers with IPv4- and IPv6-capabilities. Our approach, described below, borrows from the work of Hendricks et al. [18] who identified IPv6 open resolvers to measure the potential for IPv6-based DDoS attacks.

Creating control domains. We begin by creating two new domains, owned and controlled by us and used exclusively for this study. The Name Servers for each domain were also controlled by us. The Name Server for one of these domains was hosted on an IPv6-only network without the capability of communicating with IPv4. Note that because these domains were newly registered, they could not have been present on the blocklists of any censor. We refer to these domains as our control and and IPv6-only NS domains.

Identifying IPv4-capable resolvers. We then use `zmap` [15] to scan the entire IPv4 address space and issue a DNS `A` query on port 53 for our IPv4 control domain. This yields an initial list of IPv4 DNS resolvers.

Verifying IPv6 capabilities of IPv4-capable resolvers. Next, we issue a DNS `A` query for a resolver-specific subdomain of our IPv6 control domain to each of these IPv4 DNS resolvers. The subdomain encoded the IPv4 address of the resolver being targeted. Therefore, if our domain was `v6onlyNS.io` and our resolver target was `1.1.1.1`, our DNS query requested the `A` record for `1-1-1-1.v6onlyNS.io`. Since IPv4-only resolvers will not be able to communicate with our IPv6-only Name Server, we expect this resolution to fail. On the other hand, resolvers with any form of IPv6 connectivity will be able to connect to our IPv6-only Name Server. Thus, by examining the logs of our IPv6-only NS domain, we are able to identify the set of resolvers that successfully reached our server and their corresponding IPv4 addresses. The associated IPv6 address for each successful query is extracted from packet captures of the IPv6-only Name Server giving us an (IPv4, IPv6) address pair for each resolver.

Filtering and geolocating resolvers. The approach detailed above yields pairs that suggest the presence of 'infrastructure' resolvers — e.g., multiple IPv4 resolvers have the same IPv6 address associated with them. These are cases where the IPv4 resolver simply forwards requests to a dedicated multi-machine DNS infrastructure rather than performing the resolution by itself. Although this does not change the validity of our results regarding the IPv6-related inconsistencies of resolvers, we still remove these cases in order to minimize the influence of such infrastructure resolvers. Finally, to confirm the correctness of our list of IPv4/IPv6 resolver pairs, we: (1) perform a follow up scan by issuing `A` and `AAAA` requests for both our control domains using `zdns` [15] and filter out those pairs where an incorrect response was received, (2) we use the Maxmind GeoIP dataset [1] to geolocate the IPv4 and IPv6 addresses of a resolver pair and only those which belong to the same region. In total, we obtained 7,788 resolvers in 106 different countries. Table 7 illustrates how these resolvers were geographically distributed.

3.2 Selecting target domains

In order to identify inconsistencies in IPv4/IPv6-related DNS censorship we require that the domains we use are: (1) sensitive and likely to be censored in a large number of countries and (2) have valid `A` and `AAAA` records associated with them.

Identifying sensitive domains. Censored Planet's 'Satellite' project, which performs global longitudinal measurements of DNS censorship, [37] maintains a list of domains that combines sensitive domains in each country with popular domains randomly chosen from the Alexa Top-10K. The sensitive domains in this list were gathered by the Citizen Lab using regional experts to curate lists for each country [24]. Given the input from experts and the availability of comparable validation data from Censored Planet, we utilize this list as the starting point for our study as well.

Identifying usable domains. Not all the domains on the Satellite list are usable in our study since they do not have IPv6 connectivity or `AAAA` records. We filter out unusable domains by using `zdns` to perform `A` and `AAAA` resource record requests from Google and Cloudflare's four public DNS resolvers (`8.8.8.8`, `8.8.4.4`, `1.1.1.1`, and `1.0.0.1`) and removing those with invalid `A` or `AAAA` records. A record is invalid if it does not contain valid IPv4 or IPv6 addresses. Finally, we follow-up by making TLS connections (using `zgrab2`), from our uncensored vantage point, to each of the IP addresses contained in the DNS responses. We locally verify the obtained TLS certificates and exclude all domains whose verification fails. This final list contains 717 sensitive domains whose TLS certificates and IPv4 and IPv6 addresses are valid. We use this list for all the measurements reported in this paper.

3.3 Identifying DNS censorship events

In general, our goal is to err on the side of caution and avoid false-positives in our censorship determination. We achieve this by accounting for unreliability of resolvers and domains in our lists.

Removing unstable resolvers. For each of the 7,788 (IPv4, IPv6) resolver pairs and 717 sensitive domains, we send a DNS `A` and `AAAA` resource record request for a domain to the IPv4 and IPv6 addresses associated with the resolver. We follow this up with a `A` and `AAAA` resource record request for a set of 3 control domains (owned and operated by us). We discard data from resolver pairs which failed to resolve any of our control domains correctly since this is a sign of resolver instability. This left us with data from 7,428 stable resolver pairs.

Distinguishing censorship from domain instability. For the remaining resolvers, we extract the IPv4 and IPv6 resource records returned for each domain. Next, we use `zgrab2` to establish TLS connections to the IP addresses contained in the resource records. In each of these connections, we set the TLS SNI (using the `-servername` option) to be the domain whose records were requested. We then verify the validity of the retrieved TLS certificates. Since the domains themselves might be unreliable, we repeat this verification procedure three times. Only if this step fails all three times do we conclude that the response from that resolver for that domain was censored.

3.4 Ethics

Our experimental design has incorporated ethical considerations into the decision-making process at multiple stages. We concern ourselves primarily with the security and autonomy of human users and their ability to securely access the internet. Given the prevalence of self-censorship, understanding and documenting the mechanisms and scope of censorship strategies can assist users in better evaluating their own risk. However, censorship measurement naturally entails interacting with and occasionally violating the rules of access control systems. We rely on The Menlo Report [14], its companion guide [6], and the censorship specific ethical measurement guidelines discussed by Jones et al. [21] to provide structure and guidance to our experimental design.

Consent. To align with the guiding principle of *respect for persons* we structure the data collection to implicate as few individuals as possible. Specifically we rely on open resolvers which typically have little or no direct association with individuals in lieu of measurement from client based software. While we cannot acquire direct or proxy consent from the operators of the open resolvers we consider the trade-off between the implied consent standard and the value in the measurements we make. Understanding the extent and mechanisms of censorship infrastructure can help to demystify and clarify risks to real users seeking to safely access the internet. It is important to note that the goal of our ethical analysis is not to eliminate risk, but to minimize it wherever possible. As noted by Jones et al. in some cases acquiring consent from operators may not only be impossible, but increase the risk to operators as it introduces their acknowledgement of, or active participation in, the measurement at hand [21]. This analysis aligns with previous work relying on open resolvers to collect impactful results while minimizing risk on individuals [33, 35, 37].

Privacy. Our study collects no personal data about any end users or individual open resolver operators. The analysis completed herein uses resolver addresses, public Anonymous System (AS) identifiers, and country codes. All measurements are initiated from within the United States at little to no risk of repercussions to citizens in the countries that we examine. Beyond this, measurement domains are not drawn from any human browsing patterns or history as the suspected censored domains are a subset of the Satellite measurement results as discussed in §3.2.

Resource usage. The vantage that was used for data collection is connected to the internet with a 1 Gbps interface that scanned using the default rates for `zmap` and `zgrab2` tools (line rate). However, the structure of the scan was established such that individual resolvers and domains for the DNS probe and TLS certificate validation respectively would be accessed in round robin order — i.e., when probing the open resolvers every target would receive a preliminary request before any target would receive the subsequent request. Equivalently for validating TLS certificates, each of the 717 target domains would receive a preliminary attempted handshake before any target would receive a subsequent handshake. While we do not have an upper bound on the bandwidth that was sent to individual resolvers or TLS endpoints we believe this strategy provides a reasonable limitation to the impact of the measurements in this study.

4 Prevalence of DNS Censorship

Overview. In this section, we focus on *providing a high-level understanding on the prevalence of DNS censorship on IPv4 and IPv6 networks*. Specifically, we measure the global prevalence of DNS censorship that occur in the following four cases: (1) a DNS `A` query is sent over IPv4, (2) a DNS `AAAA` query is sent over IPv4, (3) a DNS `A` query is sent over IPv6, and (4) a DNS `AAAA` query is sent over IPv6. While much of prior work has focused on case (1), the increased adoption of IPv6 necessitates the analysis of cases (2-4) which are provided in our work. In each case, we use our collected dataset (*cf.,* §3) to summarize the base rate of censorship.

Country	**Resolver pairs**	**IPv4** `A`	**IPv4** `AAAA`	**IPv6** `A`	**IPv6** `AAAA`	**Avg.**
China (CN)	194	29.27	32.32	28.41	32.08	30.52
Iran (IR)	277	25.12	24.49	21.95	21.45	23.25
Hong Kong (HK)	67	7.00	5.57	4.91	5.24	5.68
Russia (RU)	312	5.51	4.78	4.49	4.50	4.82
Ukraine (UA)	35	6.49	3.05	2.64	2.87	3.76
Indonesia (ID)	56	6.46	2.99	2.41	2.26	3.53
Argentina (AR)	47	5.20	3.51	2.22	1.28	3.05
Thailand (TH)	186	8.25	1.18	1.13	0.93	2.87
Malaysia (MY)	50	4.92	2.03	1.27	1.35	2.39
Mexico (MX)	150	3.78	2.05	1.75	1.94	2.38
Bangladesh (BD)	29	6.42	1.28	0.89	0.81	2.35
Colombia (CO)	27	3.39	3.28	1.45	1.14	2.31
Italy (IT)	38	2.36	2.10	2.25	2.52	2.31
Brazil (BR)	160	2.67	1.67	1.99	2.08	2.10
Bulgaria (BG)	30	3.24	2.91	1.15	1.06	2.09
Poland (PL)	48	2.00	1.13	2.90	0.96	1.75
South Africa (ZA)	93	2.41	1.60	1.18	1.33	1.63
Korea (KR)	632	2.33	1.06	1.24	1.22	1.46
Chile (CL)	65	2.67	0.70	1.10	0.79	1.32
Romania (RO)	44	2.30	1.03	0.83	0.93	1.27
Spain (ES)	49	0.91	0.75	1.40	1.94	1.25
India (IN)	226	1.27	1.52	1.04	1.16	1.25
Belgium (BE)	31	1.56	1.26	0.95	0.95	1.18
Turkey (TR)	114	1.29	0.96	1.27	1.02	1.14
Viet Nam (VN)	252	1.53	0.89	1.42	0.67	1.13
Global	7,428	3.10	1.83	1.77	1.60	2.07

Table 1: Top-25 countries with over 25 resolver pairs and the highest average rates of DNS censorship across both query types and network interfaces. Rates are expressed as the percentage of censored DNS queries over total number of DNS queries sent. Darker shaded cells indicate a higher rate of DNS censorship (compared to the country's average) and lighter shaded cells indicate a lower rate of DNS censorship. The average rate of censorship for a country is computed across all four IP/query combinations. The global row contains the mean of each column and includes data from the countries with less than 25 resolvers. These means weigh the contribution of each country equally, rather than weighted by the number of resolvers used in tests. Countries are grouped together by their distance from this median.

How common is DNS censorship? Our data shows the mean base rate of DNS censorship among the 106 countries included in our study, across all query and network types, for our list of domains is 2.1%. A summary of the base rates observed in each of our four `A`/`AAAA`-IPv4/IPv6 combinations for the 25 countries which have at least 25 pairs of resolvers that were tested and perform the most censorship is illustrated in Table 1. In general, our results concur with prior work which has also found high levels of DNS censorship in China, Iran, Russia, and Hong Kong.

Trends in censorship of IPv6-related queries in heavily censoring countries. By measuring IPv6-related behaviors of censorship mechanisms, we uncover a large number of DNS censorship inconsistencies in heavily censoring countries. Because our dataset is balanced (i.e., all the domains

Country	Resolver Pairs	IPv4 A	IPv4 AAAA	IPv6 A	IPv6 AAAA	Avg.
United States (US)	757	1.62	1.16	0.54	0.96	1.07
Germany (DE)	717	0.98	0.91	0.75	0.80	0.86
France (FR)	470	0.60	0.45	0.40	0.46	0.48
Great Britan (GB)	186	1.07	0.94	0.78	0.97	0.94
South Korea (KR)	177	2.49	1.37	1.38	1.57	1.70
Canada (CA)	165	0.84	0.39	0.26	0.33	0.45
Russia (RU)	117	4.67	4.36	4.01	4.00	4.26
India (IN)	101	1.19	1.76	0.81	0.99	1.19
Japan (JP)	79	1.71	1.82	0.90	1.57	1.50
South Africa (ZA)	74	2.09	1.62	1.10	1.31	1.53
Netherlands (NL)	71	1.08	0.94	0.84	0.85	0.92
Chile (CL)	53	2.10	0.73	1.12	0.77	1.18
Lithuania (LT)	51	0.95	0.80	0.51	0.78	0.76
Iran (IR)	48	25.50	24.66	22.34	21.69	23.55
Thailand (TH)	43	9.28	1.18	0.99	0.95	3.10
Singapore (SG)	41	1.56	0.85	0.65	0.78	0.96
Viet Nam (VN)	40	2.16	1.01	0.85	0.86	1.22
Hong Kong (HK)	37	6.20	5.44	4.55	5.38	5.39
Austrailia (AU)	35	2.53	1.16	1.77	1.14	1.65
Brazil (BR)	34	1.50	1.10	1.01	1.17	1.19
Finland (FI)	31	0.74	0.64	0.47	0.56	0.60
Malaysia (MY)	30	6.07	2.25	0.97	1.10	2.60
Spain (ES)	28	1.26	0.97	2.24	2.97	1.86
Turkey (TR)	25	1.72	1.29	1.20	2.17	1.60

Table 2: We highlight the countries with at least 25 resolver pairs in corporate ASes to showcase their censorship rates across interface and resource type. We see this is where the predominant censorship in the United States is present.

have both `A` and `AAAA` records and all the tested resolvers have an IPv4 and IPv6 interface), if censorship is independent of the query type and interface, we expect to see a uniform rate of censorship across all query types and interface combinations in Table 1. However, we find that this is not true. We observe two trends common to many of the countries performing the most censorship. First, we see that, in comparison to any other query-interface combination, `A` *queries sent over IPv4 are the most heavily censored*. Second, we see that `AAAA` *queries are censored less than* `A` *queries, regardless of whether they are sent over IPv4 and IPv6 networks*. This immediately suggests that censorship apparatus in a large number of censoring regions are not fully IPv6-capable. Besides the possibility of misconfiguration of the DNS censorship mechanisms, this may also be because censors in these regions are not yet widely deployed on IPv6 networks in their country. The only exception to both these generalizations is China — the most censoring country in our data. China shows an unusual *preference towards blocking* `AAAA` *records regardless of whether they are sent over IPv4 or IPv6*. We explore China and several other countries with interesting patterns as specific case studies in §7.

Corporate Censorship. Predominantly the focus of DNS censorship is at the nation state level as discussed so far. However, corporate censorship i.e., businesses restricting employee access to certain domains is also highly prevalent across the internet.

Given our wide breadth of resolvers we were able to break down our resolver pairs discovered (as discussed in §3.1) further into the the Autonomous System (AS) each resolver pair is in allowing us to get a more fine grained look at which resolvers are censoring access to sensitive domains.

Table 2 shows the censorship rates across resource and infrastructure type in countries that had at least 25 resolver pairs in corporate ASes.

5 Censorship of IPv4 and IPv6 Resource Records

Overview. In this section, we focus on *identifying and characterizing differences in the handling of IPv4 and IPv6 resource records* in DNS censorship deployments. Specifically, we seek to answer the following questions: (§5.1) In which countries is the censorship of IPv4 **resource records** (DNS `A` queries) significantly different than the censorship of IPv6 resource records (DNS `AAAA` queries)?, (§5.2) what are the characteristics of the **resolvers** which exhibit differences in the handling of `A` and `AAAA` queries?, and (§5.3) what are the characteristics of **domains** in which these differences are frequently observed?

5.1 `A` vs. `AAAA` resource censorship

We use the responses received from our `A` and `AAAA` queries sent to the same set of resolvers and for the same set of domains (*cf.,* §3 for data collection methodology). We then apply the censorship determination methods described in §3.3 to measure the prevalence of censorship on our `A` and `AAAA` DNS queries. Finally, we perform statistical tests to identify significant differences in the prevalence of censorship of `A` and `AAAA` queries within each country.

Identifying differences within a country. To measure differences in DNS query handling within a specific country, we compare the prevalence of censorship on `A` and `AAAA` queries by aggregating responses across each resolver within the country. This presents us with two distributions (one each for the group of `A` and `AAAA` queries) of the fraction of censored domains observed at each resolver in the country. We use a two-sample t-test to verify statistical significance of any observed differences between the two groups for each country. In our statistical analysis, we aim to achieve a significance level of 5% ($p \leq .05$) *over all our findings*. Therefore, we apply a Sidak correction [3] to control for Type I (false-positive) errors from multiple hypothesis testing. This requires $p \leq 1 - .05^{1/n_c}$ for classifying a difference as significant, where n_c is the total number of countries in our dataset (106). This approach reduces the likelihood of false-positive reports of within-country differences. The presence of a statistically significant difference for a specific country would imply that `A` and `AAAA` resource types appear to undergo different censorship mechanisms within that country (if a centralized mechanism for censorship exists) or that a significant number of resolvers within that country have inconsistencies in their censoring of each query type. A summary of our results are presented in Table 3.

Country	IPv4 resolvers	IPv6 resolvers	All resolvers
Thailand (TH)	-7.1 pp (-85.7%)	*ns*	-3.7 pp (-77.5%)
Bangladesh (BD)	-5.1 pp (-80.0%)	*ns*	-2.6 pp (-71.3%)
Pakistan (PK)	-2.1 pp (-73.6%)	-2.8 pp (-59.8%)	-2.5 pp (-60.2%)
Chile (CL)	-2.0 pp (-57.6%)	*ns*	-1.1 pp (-58.9%)
Vietnam (VN)	*ns*	-0.7 pp (-52.5%)	-0.7 pp (-47.1%)
Korea (KR)	-1.3 pp (-54.6%)	*ns*	-0.6 pp (-36.2%)
China (CN)	3.1 pp (+10.4%)	3.7 pp (+12.9%)	3.4 pp (+11.7%)
United States (US)	-0.5 pp (-33.2%)	0.4 pp (+72.3%)	*ns*
Myanmar (MY)	-2.9 pp (-58.9%)	*ns*	*ns*

Table 3: Differences in blocking rates of A and AAAA queries observed over IPv4, IPv6, and all resolvers in a country. 'pp' denotes the change in terms of percentage points (computed as AAAA blocking rate - A blocking rate) and the %age value denotes the percentage change in blocking rate (computed as $100 \times \frac{\texttt{AAAA}\text{ blocking rate}-\texttt{A}\text{ blocking rate}}{\texttt{A}\text{ blocking rate}}$). Only countries having a statistically significant difference are reported. A negative value indicates that A queries observed higher blocking rates than AAAA queries. *ns* indicates the difference was not statistically significant and thus omitted.

How many countries demonstrate large-scale inconsistencies in their handling of A and AAAA queries? In total, only seven countries showed a statistically significant difference in the rate at which AAAA and A DNS requests were blocked. We note that this is a conservative lower-bound due to the statistical test used, which minimizes false positive errors at the expense of false negatives. This finding suggests the presence of independent censorship mechanisms for handling each query type in the seven countries (Thailand, Bangladesh, Pakistan, Chile, Vietnam, Korea, and China). Of these, six (China being the only exception) were found to have lower blocking rates for AAAA queries than A queries. In fact, the AAAA censorship rates were between 36-78% lower than the A censorship rate suggesting that their censorship mechanisms for AAAA queries that are associated with IPv6 connectivity are still lagging. Further analysis shows that the differences are mostly found on the IPv4 interfaces of our resolvers (*cf., IPv4 resolvers* column in Table 3) where the AAAA censorship rates were up to 86% lower than the A censorship rates. This finding is indicative of a tendency for network operators to have focused efforts on maintaining infrastructure for censoring A queries sent to IPv4 resolvers, while paying less attention to the handling of AAAA queries and their IPv6 interfaces. It also presents an opportunity for circumvention tool developers to exploit. China presents the only exception with a preference for blocking AAAA queries on both IPv4 and IPv6 interfaces of resolvers with a 10% and 13% higher AAAA censorship rate, respectively. We investigate this anomaly in §7.

5.2 Characteristics of A/AAAA-inconsistent resolvers

Given our above results which suggest that there are a number of countries in which A and AAAA queries are censored differently, we now seek to understand the characteristics of the resolvers that cause these differences. We first focus on identifying the individual resolvers in each country that have statistically different behaviors for A and AAAA queries. Then, we compare the AS distributions of these resolvers with the set of all resolvers in a country. This comparison tells us if the A/AAAA inconsistencies are specific to a subset of ISPs, or if the inconsistencies exist across the whole country (suggesting centralized censorship). Finally, we identify the types of networks hosting inconsistent resolvers to get a measure of whether users in residential networks may exploit these DNS inconsistencies for circumvention.

Identifying differences in individual resolvers. We begin our analysis by identifying the individual resolver pairs (i.e., we consider the IPv4- and IPv6-interfaces of a resolver as a unit), within each of the seven countries listed above that have a statistically significant difference in their censorship of A and AAAA queries. To measure differences in DNS query handling of individual resolvers, we compare the ratio of censored responses each resolver observes for A and AAAA queries.

We use a two-proportion z-test to verify the statistical significance of any observed difference in the ratios between the two groups for each resolver. Similar to our within-country analysis, we apply a Sidak correction to account for our testing of multiple hypotheses and use $p \leq 1 - .05^{1/n_{rc}}$ to classify a difference as significant, where n_{r_c} is the total number of resolvers in our dataset belonging to country c. A summary of our results is provided in Table 4.

Which countries have the largest fractions of resolvers exhibiting A and AAAA resolution inconsistencies? Immediately standing out from the other countries are Thailand, Bangladesh, and Pakistan. These countries have A and AAAA inconsistencies in 62-82% of their resolvers. In comparison, other countries with statistically significant differences have inconsistencies arising from anywhere between 3-30% of their resolvers.

How spread out are the A/AAAA-inconsistent resolvers? We calculate the entropy of the distribution of all resolvers in the country ($S^{\text{all}}_{\text{query}}$) and compare it with the entropy of the distribution of the inconsistent resolvers in the country ($S^{\text{inconsistent}}_{\text{query}}$). This serves as a measure of the diversity of ASes observed in both cases. In order to compare the two measures, we use the Kullback-Leibler divergence (∇_{query}) distance [23]. In simple terms, the KL-divergence between two distributions (X, Y) measures the number of additional bits required to encode X given the optimal encoding for Y. In other words, it is the relative entropy of one distribution given another. This computation is helpful for hypothesizing the censorship infrastructure that causes the inconsistencies. Finding a small ∇_{query} value in a country signifies that the inconsistent resolvers had a similar distribution to all the resolvers in that country. This would suggest the presence of a centralized mechanism that (roughly) equally impacts all ASes in the country that is responsible for the inconsistencies. Conversely, a higher ∇_{query} value indicates that there is a strong change in the distribution of resolvers – i.e., a disproportionate number of inconsistencies arise from a smaller set of ASes. This would be indicative of local configuration inconsistency (at the network or resolver level), rather than a centralized configuration inconsistency. We note that this does not provide a measure of how centralized censorship is within a country overall, but rather, it describes how uniform the `A` vs. `AAAA` inconsistencies are.

Based on this analysis, we once again see that Thailand, Bangladesh, and Pakistan stand out with small ∇_{query} values (0.14 - 0.48). This suggests a country-wide censorship mechanism is responsible for the inconsistent censorship of `A` and `AAAA` that impacts all ASes nearly equally. Korea, China, and the United States on the other hand demonstrate high ∇_{query} scores suggesting the presence of network- or resolver-level misconfigurations are responsible. This is confirmed by inspecting the ASes hosting the resolvers with inconsistencies. For example, in the United States, resolvers in just 5 ASes (of 249 ASes with resolvers) account for 56% of all `A` and `AAAA` inconsistencies.

What types of networks exhibit the most `A` and `AAAA` inconsistencies? We use the Maxmind GeoIP2 connection type database (retrieved in 01/2022 [1]) to identify the connection type of the resolvers responsible for `A` and `AAAA` inconsistencies. We find that, in most countries, Cable/DSL network connections (typically associated with residential networks) were most likely to host a resolver exhibiting an inconsistency. Of the seven countries with statistically significant overall differences, only Thailand and China were found to have a high ratio of `A/AAAA` -inconsistent resolvers in corporate networks. Combined with our previous results which suggest the presence of an inconsistency in a centralized mechanism in Thailand, Bangladesh, and Pakistan, these results show that these inconsistencies are likely extending to residential networks — a promising sign for the citizen users of circumvention tools which exploit the `A/AAAA` gap.

5.3 Characteristics of anomalous domains

We now identify the category of domains that appear to exist in the gap of `A` and `AAAA` blocking. In addition to providing a general categorization of these domains, we also analyze whether their category distributions vary significantly from the category distribution of websites that received any blocking. We do this in order to identify the specific policies or mechanisms that differ between the censorship mechanisms for `A` and `AAAA` queries.

Identifying differences in domain behaviors within a country. We continue using our statistical approach for identifying differences within a country. We measure the ratio of blocking that occurs for a domain's `A` and `AAAA` records within the country and then compare these using a two-proportion z-test with a Sidak corrected p-value of $1-.05^{dom}$ where dom is the total number of tested domains (717). We only label the behavior of a censor with regards to a domain as different over `A` and `AAAA` queries if the z-test finds the difference to be statistically significant. Once again, we do this to err on the side of caution in order to minimize over-reporting and false-positives of censorship and, in this case, its corresponding policy differences over `A` and `AAAA`.

Do these `A/AAAA`-inconsistent domains hint at policy gaps? For each country, we begin our analysis by deriving domain categories, using the McAfee domain categorization service [**?**], for domains in the following two lists: (1) D_{any} which contains the domains which experienced any blocking events inside a country and (2) $\text{D}_{\text{inconsistent}}$ which contains the `A/AAAA`-inconsistent domains identified by our z-test. Next, we compute the KL-divergence between the category distributions of the two lists (i.e., $\nabla_{\text{query}}^{\text{domains}} = \text{KLDivergence}(\text{D}_{\text{any}}, \text{D}_{\text{inconsistent}})$). A small $\nabla_{\text{query}}^{\text{domains}}$ would signify that the domains that experience inconsistent treatment are not from a largely different category distribution than the set of all domains that experience any type of blocking. This would suggest that the inconsistencies do not arise from a specific content-specific policy gap that exists in the censorship mechanism implemented over `A` and `AAAA` queries. On the other hand, a large difference would signify that the category distributions are very different and that domains with specific types of content appear to have more inconsistencies — suggesting a content-based policy gap.

Based on this analysis, we find that the United States and Thailand have the smallest $\nabla_{\text{query}}^{\text{domains}}$ scores (0.4-1.2). Conversely, Pakistan and Myanmar have high $\nabla_{\text{query}}^{\text{domains}}$ scores (>2). After manual inspection of these results, we attribute the low divergence in the United States to the fact that censorship observed in the US arise largely in a range of corporate networks (§4) which are fairly consistent in their blocking of domains belonging to McAfee's 'Potentially unwanted programs', 'Entertainment', and 'Pornography' categories. On the other hand, in Thailand the low divergence appears despite the large number of residential networks. This suggests that there is no significant policy gap that causes the `A/AAAA`-inconsistencies. Rather, it suggests a simply incomplete implementation of any existing mechanisms for `A` query censorship. On the other hand, in Pakistan and Myanmar where the divergence scores were high, we found that the biggest contribution to the high divergence scores arose from the 'Pornography' and 'Government/Military' domain categories, respectively. This suggests the presence of a content-policy gap in the implementation of `A/AAAA` DNS censorship implementations that disproportionately allows sites in these categories to evade censorship.

Country	Total pairs	Inconsistent pairs	Most inconsistent AS	AS diversity			Most inconsistent type
		(% of total pairs)	(# inconsistent pairs)	$S^{\text{all}}_{\text{query}}$	$S^{\text{inconsistent}}_{\text{query}}$	∇_{query}	(# inconsistent pairs)
Thailand (TH)	186	152 (81.7%)	AS9835 Government IT Services (40)	4.50	4.06	0.14	Cable/DSL (110)
Bangladesh (BD)	29	18 (62.1%)	AS 9230 Bangladesh Online (4)	4.10	3.61	0.48	Cable/DSL (18)
Pakistan (PK)	23	15 (65.2%)	AS 17911 Brain Telecom (3)	3.43	3.06	0.25	Cable/DSL (12)
Chile (CL)	65	20 (30.1%)	AS 27651 Entel Chile (13)	3.08	1.14	1.18	Corporate (13)
Vietnam (VN)	252	64 (25.4%)	AS 131353 NhanHoa Software (37)	3.89	2.22	0.71	Cable/DSL (59)
Korea (KR)	632	80 (12.7%)	AS 9848 Sejong Telecom (13)	3.12	4.17	1.30	Cable/DSL (58)
China (CN)	194	6 (3.1%)	AS 4538 China Education and Research Network (2)	3.89	2.25	2.56	Corporate (4)
United States (US)	1,228	175 (14.3%)	AS 30475 WEHOSTWEBSITES (35)	6.28	4.69	1.31	Corporate (129)
Myanmar (MY)	50	30 (60%)	AS 136170 Exabytes Network (10)	3.31	2.42	0.48	Corporate (26)

Table 4: Characteristics of the resolvers which demonstrated a statistically significant difference in their handling of `A` and `AAAA` queries in each country. 'AS diversity' denotes the entropies of (all) resolver distribution ($S^{\text{all}}_{\text{query}}$) and `A/AAAA`-inconsistent resolver distribution ($S^{\text{inconsistent}}_{\text{query}}$) across a country's ASes, and '∇_{query}' represents the Kullback-Leibler divergence of the distribution of inconsistent resolvers from the distribution of all resolvers in the country's ASes (*cf.,* §5.2). 'Most inconsistent type' denotes the connection type with the most number of `A/AAAA`-inconsistent resolvers.

6 Censorship of IPv4 and IPv6 DNS Traffic

Overview. In this section, we focus on *identifying and characterizing the differences in handling DNS queries sent over IPv4 and IPv6 networks* in DNS censorship mechanisms. Specifically, we answer the following questions: (§6.1) In which countries are the DNS censorship mechanisms for IPv4 and IPv6 traffic significantly different?, (§6.2) what are the characteristics of resolvers that exhibit differences in the censorship of IPv4 and IPv6 traffic?, and (§6.3) what are the characteristics of the domains in which such differences are frequently exhibited?

6.1 Within-country differences in the censorship of IPv4 and IPv6 DNS queries

We use the responses received from the IPv4 and IPv6 interfaces of each of the resolvers in our dataset for the same set of domains. We then apply the censorship detection mechanism detailed in §3.3 to measure the prevalence of DNS censorship of queries sent over IPv4 and IPv6. Finally, we perform statistical tests to identify the countries that have significant differences in their censorship of IPv4 and IPv6 DNS traffic.

Identifying differences within a country. To measure differences in the censorship of DNS queries sent over IPv4 and IPv6, we compare the prevalence of censorship on each by aggregating their responses across each resolver within a country. This presents us with two distributions (corresponding to the IPv4 and IPv6 interfaces of resolvers) of the fraction of censored domains from resolvers within the corresponding country. We use a two-sample t-test to verify statistical significance of any observed differences between the two groups for each country. Similar to our approach in §5, we apply a Sidak correction to control for Type I errors from multiple hypothesis testing. This requires $p \leq 1 - .05^{1/n_c}$ for classifying a difference as significant, where n_c is the total number of countries in our dataset (106). The presence of a statistically significant difference for a specific country would imply that the country appears to have different censorship mechanisms for IPv4 and IPv6 DNS traffic (if a centralized mechanism for censorship exists) or that a significant number of resolvers within that country are not consistent in their censorship of IPv6 and IPv4 traffic. A summary of our results are presented in Table 5.

Which countries demonstrate large-scale inconsistencies in their handling of IPv4 and IPv6 DNS traffic? In total, we find only five countries (Thailand, Iran, Bangladesh, Myanmar, and the United States) with statistically significant differences in their handling of DNS queries over IPv4 and IPv6 traffic — suggesting the use of independent censorship mechanisms for IPv4 and IPv6. Interestingly, all these countries appear to have gaps in their IPv6 censorship apparatus — i.e., IPv4 rates of blocking are higher than IPv6 rates in all countries with significant differences. These differences result in IPv6 queries experiencing between 12% and 78% less censorship than their IPv4 counterparts. Once again, this suggests a tendency for network operators to more effectively maintain IPv4 DNS censorship infrastructure than IPv6 infrastructure. These gaps present opportunities for the success of circumvention tools with IPv6 capabilities. Further analysis shows that these differences primarily arise due to the fact that DNS type `A` queries are significantly more likely to be blocked over IPv4 connections than over an IPv6 connection. However, this is not the case for `AAAA` queries, with the exception of Iran. Taken together, these findings are particularly noteworthy for circumvention efforts in Thailand, Myanmar, and Iran where IPv6 adoption rates are high (between 15% and 45%) and dual-stack tools may be used for circumvention of DNS censorship.

Country	A queries	AAAA queries	All queries
Thailand (TH)	-7.1 pp (-86.3%)	*ns*	-3.7 pp (-78.1%)
Iran (IR)	-3.2 pp (-12.6%)	-3.0 pp (-12.5%)	-3.1 pp (-12.5%)
Bangladesh (BD)	-5.5 pp (-86.1%)	*ns*	-3.0 pp (-77.9%)
Myanmar (MY)	-3.6 pp (-74.2%)	*ns*	-2.1 pp (-62.3%)
United States (US)	-0.9 pp (-64.8%)	*ns*	-0.5 pp (-42.6%)
Korea (KR)	-1.1pp (-46.5%)	*ns*	*ns*
Chile (CL)	-1.6pp (-58.7%)	*ns*	*ns*

Table 5: Differences in blocking rates of DNS queries sent to IPv4 and IPv6 interfaces of each resolver in a country. 'pp' denotes the change in terms of percentage points (computed as blocking rate of IPv6 - blocking rate of IPv4) and the %age value denotes the percentage change in blocking rate (computed as $100 \times \frac{\text{IPv6 blocking rate}-\text{IPv4 blocking rate}}{\text{IPv4 blocking rate}}$). Only countries having a statistically significant difference are reported. A negative value indicates that queries sent over IPv4 observed higher blocking rates than those sent over IPv6. *ns* indicates the difference was not statistically significant and thus omitted.

6.2 Characteristics of IPv4/IPv6-inconsistent resolvers

Our previous results demonstrate the promise of using IPv6 channels for DNS resolution to bypass IPv4 DNS censorship. We now focus on identifying the distribution and connection-type of resolvers demonstrating inconsistencies in their handling of IPv4 and IPv6 traffic. This serves two purposes. First, our analysis on the distribution of IPv4/IPv6-inconsistent resolvers provides evidence-driven hypotheses about how information controls deployments are structured in different countries. Second, studying the connection-types of IPv4/IPv6-inconsistent resolvers sheds light on whether the gaps in censorship are visible to users in residential networks. This serves as an indicator for the potential gains to be had by circumvention tools that begin exploiting the IPv4/IPv6 gap.

Identifying IPv4/IPv6-inconsistent resolvers. Our approach is similar to the methods used to identify A/AAAA-inconsistent resolvers (*cf.,* §5.2). We compare the ratios of censored responses received from a single resolver pair's IPv4 and IPv6 interfaces. We test whether these ratios are statistically different using a z-test with a Sidak corrected $p \leq 1 - .05^{1/n_{rc}}$ being required for a statistically significant difference. A summary of the characteristics of the inconsistent resolvers identified in each country is illustrated in Table 6.

Which countries have the largest fraction of IPv4/IPv6-inconsistent resolvers? Two countries from our previous analysis on A/AAAA-inconsistencies once again appear with a large fraction of IPv4/IPv6-inconsistent resolvers — Thailand (81%) and Bangladesh (65%). Myanmar presents a new addition with 60% of its resolvers demonstrating IPv4/IPv6-inconsistencies. Other countries were found to have smaller fractions ranging from 12-26%.

How spread out are the IPv4/IPv6-inconsistent resolvers? In order to characterize the spread of IPv4/IPv6-inconsistent resolvers within a country, we compute the entropy of the AS distribution of all resolvers and IPv4/IPv6-inconsistent resolvers within a country ($S^{\text{all}}_{\text{net}}$ and $S^{\text{inconsistent}}_{\text{net}}$) and then compute the KL-divergence of the distribution of inconsistent resolvers from the distribution of all resolvers in that country (∇_{net}). Similar to before, a large change in ∇_{net} means that the IPv4/IPv6-inconsistencies arise from a small fraction of ASes and would suggest that the gaps exist due to local network/resolver misconfigurations — as would be the case if regional operators implement their own DNS censorship mechanisms. Conversely, a small change means that the gaps that exist roughly equally impact all the ASes having resolvers and would suggest that the gaps exist due to misconfigurations in a centralized DNS censorship mechanism. Our results once again suggest the presence of a centralized blocking mechanism in Thailand, Bangladesh, and Myanmar ($\nabla_{net} \in [0.13, 0.48]$) which causes the IPv4/IPv6-inconsistencies. The United States has the highest ∇_{net} observed which indicates that regional policies are responsible for the IPv4/IPv6-inconsistencies.

What types of networks exhibit the most IPv4 and IPv6 inconsistencies? An overwhelming majority of the inconsistent resolvers in Thailand, Iran, and Bangladesh (77%-100%) are found to be present in networks with (Maxmind categorized) Cable/DSL connection-types that are typically associated with residential networks. Put in the context of our previous result which suggests the presence of a centralized DNS censorship mechanism in Thailand and Bangladesh, this suggests that the IPv4/IPv6 gaps that exist in this mechanism also extend to residential networks in the country. Myanmar and the United States experience such inconsistencies primarily due to their corporate networks which contain between 67-87% of their inconsistent resolvers.

6.3 Characterization of anomalous domains

We now seek to understand the category of domains that get through the infrastructural gap between DNS queries over IPv4 and IPv6. We provide a general categorization of these domains and further compare this category distribution with that of domains that received any blocking. We do this in order to identify specific mechanisms that might differ for censorship of certain categories over IPv4 and IPv6.

Identifying differences in domain behaviors within a country We use an approach similar to the one defined in §5.3 for identifying domains that get through the gap in between IPv4 and IPv6. For each domain, we measure the ratio of blocking that occurs over IPv4 and IPv6. We then apply the z-test with a corrected p-value (as described in §5.3) to these ratios. This gives us all domains which had significant differences in censorship over IPv4 and IPv6.

Country	**Total pairs**	**Inconsistent pairs**	**Most inconsistent AS**	**AS diversity**			**Most inconsistent type**
		(% of total pairs)	(# inconsistent pairs)	$S_{\text{net}}^{\text{all}}$	$S_{\text{net}}^{\text{inconsistent}}$	∇_{net}	(# inconsistent pairs)
Thailand (TH)	186	151 (81.2%)	AS 9835 Government IT Services (39)	4.50	4.10	0.13	Cable/DSL (108)
Iran (IR)	277	74 (26.7%)	AS 208161 PARSVDS (11)	5.03	3.81	0.87	Cable/DSL (57)
Bangladesh (BD)	29	19 (65.2%)	AS 9230 Bangladesh Online (4)	4.10	3.72	0.39	Cable/DSL (19)
Myanmar (MY)	50	30 (60.0%)	AS 136170 Exabytes Network (10)	3.31	2.42	0.48	Corporate (26)
United States (US)	1,228	151 (12.3%)	AS 30457 WEHOSTWEBSITES (36)	6.28	5.22	1.44	Corporate (102)
Korea (KR)	632	101 (16.0%)	AS 9848 Sejong Telecom (13)	3.12	4.14	0.95	Cable/DSL (73)
Chile (CL)	65	16 (24.6%)	AS 27651 Entel Chile (12)	3.08	1.19	1.04	Corporate (11)

Table 6: Characteristics of the resolvers which demonstrated a statistically significant difference in their handling of DNS queries over IPv4 and IPv6 each country. 'AS diversity' denotes the entropies of (all) resolver distribution ($S_{\text{net}}^{\text{all}}$) and IPv4/IPv6-inconsistent resolver distribution ($S_{\text{net}}^{\text{inconsistent}}$) across a country's ASes, and '∇_{net}' represents the Kullback-Leibler divergence of the distribution of inconsistent resolvers from the distribution of all resolvers in the country's ASes (*cf.,* §6.2). 'Most inconsistent type' denotes the connection type with the most number of IPv4/IPv6-inconsistent resolvers.

Do these IPv4/IPv6-inconsistent domains hint at policy gaps? For each country, we derive domain categories for the following two lists; (1) D_{any} which contains the domains which experienced any blocking events inside a country and (2) $D_{\text{inconsistent}}$ which contains the `IPv4/IPv6`-inconsistent domains identified by our z-test. We again used KL-divergence between to compare these two category distributions. A small $\nabla_{\text{query}}^{\text{domains}}$ would signify that the two category distributions are not largely different suggesting the policy gap over IPv4/IPv6 is not content specific; A large $\nabla_{\text{query}}^{\text{domains}}$ would signify that the category distributions are indeed very different suggesting a content-based policy gap.

Based on this analysis, we see that Bangladesh, US and Iran have the smallest $\nabla_{\text{query}}^{\text{domains}}$ scores (0-1.3) suggesting that there was little to no difference in the distribution of the two categories. This suggests that for these countries, there is no content-based policy gaps. On the other hand, Pakistan, China and Myanmar had the highest $\nabla_{\text{query}}^{\text{domains}}$ scores (2.7-4.3). These scores suggest that some categories of domains get through the IPv4/IPv6 censorship gap much more than others. "Gambling" is the category most likely to get through this gap for China and Pakistan and "Government/Military" is the most likely to get through this gap in Iran.

7 Country-Specific DNS Censorship Trends and Mechanisms

Thailand One prominent example is Thailand, where 8.2% of `A` records were blocked by IPv4 resolvers, compared to around 1% for `AAAA` records or IPv6 resolvers in the country. The reason for this is that many instances of IPv4 resolvers predominantly (or exclusively) saw blocking on only `A` records, while their IPv6 pair saw little or no blocking on either `A` or `AAAA` records. For instance, one of the larger resolvers by blocked domains had an IPv4 endpoint that blocked 240 `A` records, but only 15 `AAAA` records from our domain list. Meanwhile, its IPv6 counterpart did not block any domains (either `A` or `AAAA` records).

China China shows an unusual preference **toward** blocking `AAAA` records over `A` records. While it is known that the Great Firewall can block `AAAA` records and injects IPv6 traffic, it is not clear why it would block those records more than `A` records. Manual investigation reveals 21 domains that almost exclusively have their `AAAA` record blocked, but not their `A` record. For example, `gmail.com`'s `AAAA` record is blocked by over 95% of resolvers in China, but the corresponding `A` record for `gmail.com` is only blocked by 1% of resolvers. The other 20 domains have similar patterns, leading to China's slight preference in blocking `AAAA` records over `A` records. We do not find any instances of domains in China that are similarly exclusively blocked by `A` record but not `AAAA`.

Iran While Iran supports both IPv6 and IPv4, it is more effective at blocking IPv4 resolvers (both `A` and `AAAA` records). We find this is due to the fact that many of the IPv6 resolvers in Iran are actually **6to4 bridges**: these are IPv6 addresses that are not native IPv6, but instead an encoding of an IPv4 address. For example, sending an IPv6 packet to `2002:0102:0304::` will send the packet encapsulated in an IPv4 packet to 1.2.3.4 (at the 6to4 gateway), whose 32-bit address is encoded in the IPv6 address (`0102:0304`). However, this can result in the packet passing encapsulated past the censor, who will observe an IPv4 packet with a protocol field denoting IPv6 encapsulation, instead of the usual UDP-carrying DNS. A naive censor may ignore such packets, allowing the domain lookup through unchecked and uncensored. We observe 272 IPv6 resolvers are actually 6to4 bridges in Iran, all of which block at lower (but non-zero) rates, compared to their corresponding IPv4 resolver.

Trends We observe two general trends that apply to many censoring countries in our data. First, **IPv4 resolvers are more heavily censored than IPv6 resolvers**. This may be because censors in those regions only inspect IPv4 packets, or that censors are more widely deployed on IPv4 networks. Second, **Native record types are more heavily censored than non-native records**. In other words, an `A` record requested from an IPv4 resolver is more likely to be censored than a AAAA record from the same interface. But conversely, we find that AAAA records are also more often censored on IPv6 resolvers than A records. This could be because a censor only supports detecting AAAA records in IPv6 traffic, and only A records in IPv4.

8 Related Work

There is a significant body of previous work investigating DNS based censorship strategies which can be generally broken down along a few major fault lines. The first is duration: snapshot studies as compared with longitudinal measurements. Many initial investigations into censorship techniques and proposals for measurement methodology provide an evaluation of DNS censorship during a single snapshot in time [4, 9, 33, 35, 39]. Similarly, a snapshot can capture DNS censorship centering around a specific event like an election or social uprising [5]. Established methodology can then be used to gain perspectives on the way that censorship evolves over time as part of a longitudinal measurement [16, 19, 30, 37].

The second major fault line that studies split across is scope: studies that focus in on the DNS censorship strategies used by individual countries as contrasted with global measurement. Censorship strategies are not universal and each censor is unique to some degree. Targeted measurement studies contribute to a better understanding of block-list infrastructure [19, 34] and explain blocking phenomena [4, 9]. Global studies provide high level view on the use of DNS censorship internationally providing context and and understanding of prevalence to specific censorship techniques [30, 33, 35, 37, 39].

This work describes a methodology for collecting global measurement of IPv6 DNS censorship data and provides a snapshot analysis of several countries of interest.

Using Open Resolvers. Open DNS resolvers provide a unique vantage point from which to study the internet and a significant number of past measurement studies rely on their potentially censored traversals to measure suspect or adversarial behavior. Here we present a non-exhaustive timeline to distinguish methodology and describe primary contributions of related work relying on open resolvers over last two decades.

In 2007 Lowe et al. queried open resolvers hosted within China eliciting injected responses to characterize Chinese censorship infrastructure and strategy [26]. In 2008 Dagon et al. performed a survey of open DNS resolvers looking for resolvers that would intentionally provide incorrect or malicious DNS records relating to phishing attempts [12]. In 2012 anonymous authors focused in more closely on the explicit censorship of the GFW DNS injection and the collateral poisoning effect that it had on open resolvers around the world [25]. In 2014 Wander et al. used open resolvers to look more broadly for global poisoning of DNS resolution by any censoring country finding that spoofed addresses were leaking primarily from China and Iran [40]. Similar to Dagon et al., in 2015 Kührer et al. performed a global study of the reliability of open DNS resolution finding evidence of censorship, injected advertisements, and other suspicious or malicious behavior by returned addresses [22].

Satellite (2016) outlines a methodology for regularly discovering the set of available open resolvers and querying hosts in order to detect paths that return incorrect or inconsistent resource records [35]. Iris (2017) relies on a very similar scanning methodology but develops a set of metrics using follow-up scans and requests that allow the authors to differentiate between inconsistency, misconfiguration, and manipulation [33]. These metrics are based on things like address consistency, TLS certificate validation, HTTP content hash, geolocation, DNS PTR lookup, and AS information. These supplemental elements allow Iris to handle cases like CDNs, virtual hosting, distributed / forwarded resolution requests and more. The 2020 Censored Planet project incorporates and extends the methods of the Satellite and Iris as part of a comprehensive and longitudinal global censorship measurement study [37]. The measurement platform improves the filtering of open resolvers using a set of trusted resolvers as a base of truth and validates TLS certificates for returned resource records. However as with Satellite and Iris, resolvers are discovered using zmap, limiting the measurement to the IPv4 address space.

IPv6 Censorship Measurement. Previous censorship studies primarily focus on measurements in IPv4 assuming that the mechanisms and block-lists are largely equivalent or finding that results were close enough to be considered noise relative to the independent question at hand. However, several efforts explicitly cover IPv6 results.

In March 2020 Hoang et al. began collection of DNS records injected by the GFW in order to classify the addresses provided, block-pages injected, and the set of hostnames that receive injections [19]. Their analysis investigates the commonality of addresses injected by the GFW, finding that all injected AAAA responses are drawn from the reserved teredo subnet 2001::/32. The longitudinal study does not directly compare the injection rates of A vs AAAA or differences in injection to DNS queries sent over IPv4 versus IPv6.

A 2021 investigation of HTTP keyword block-lists associated with the GFW found that results are largely the same between IPv4 and IPv6 [41]. However, the authors note that the GFW failed to apply the temporary 90 second "penalty box" blocking subsequent connections between the two hosts described by numerous previous studies [8, 42]. This supports our finding that for now the GFW infrastructure supporting IPv4 and IPv6 are implemented and/or deployed independently.

9 Discussion and Conclusions

References

[1] GeoIP2 Connection Type Database | MaxMind. https://www.maxmind.com/en/geoip2-connection-type-database.

[2] IPv6 Google Statistics | Google. https://www.google.com/intl/en/ipv6/statistics.html, 2022. Accessed: 2022-01-25.

[3] Hervé Abdi et al. Bonferroni and šidák corrections for multiple comparisons. *Encyclopedia of measurement and statistics*, 3:103–107, 2007.

[4] Anonymous, Arian Akhavan Niaki, Nguyen Phong Hoang, Phillipa Gill, and Amir Houmansadr. Triplet censors: Demystifying great firewall's DNS censorship behavior. In *Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet*, FOCI '20, 2020.

[5] Simurgh Aryan, Homa Aryan, and J Alex Halderman. Internet censorship in iran: A first look. In *3rd {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 13)*, 2013.

[6] M. Bailey, D. Dittrich, and E. Kenneally. Applying ethical principles to information and communication technology research. Technical report, U.S. Department of Homeland Security, 2013-10.

[7] Jan Beznazwy and Amir Houmansadr. How china detects and blocks shadowsocks. In *Proceedings of the ACM Internet Measurement Conference*, pages 111–124, 2020.

[8] Richard Clayton, Steven J Murdoch, and Robert NM Watson. Ignoring the great firewall of china. In *International Workshop on Privacy Enhancing Technologies*, pages 20–35. Springer, 2006.

[9] Global Internet Freedom Consortium et al. The great firewall revealed. http://www.internetfreedom.org/files/WhitePaper/ChinaGreatFirewallRevealed.pdf, 2002.

[10] Jakub Czyz, Mark Allman, Jing Zhang, Scott Iekel-Johnson, Eric Osterweil, and Michael Bailey. Measuring ipv6 adoption. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, pages 87–98, New York, NY, USA, 2014. ACM.

[11] Jakub Czyz, Matthew J. Luckie, Mark Allman, and Michael Bailey. Don't forget to lock the back door! A characterization of ipv6 network security policy. In *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*, 2016.

[12] David Dagon, Chris Lee, Wenke Lee, and Niels Provos. Corrupted dns resolution paths: The rise of a malicious resolution authority. 2008.

[13] Amogh Dhamdhere, Matthew Luckie, Bradley Huffaker, kc claffy, Ahmed Elmokashfi, and Emile Aben. Measuring the Deployment of IPv6: Topology, Routing and Performance. In *Proceedings of the 2012 Internet Measurement Conference*, IMC '12, pages 537–550, New York, NY, USA, 2012. ACM.

[14] D. Dittrich and E. Kenneally. The menlo report: Ethical principles guiding information and communication technology research. Technical report, U.S. Department of Homeland Security, 2012-08.

[15] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Zmap: Fast internet-wide scanning and its security applications. In *In Proceedings of the 22nd USENIX Security Symposium*, 2013.

[16] Arturo Filasto and Jacob Appelbaum. Ooni: Open observatory of network interference. In *FOCI*, 2012.

[17] Genevieve Gebhart and Tadayoshi Kohno. Internet censorship in thailand: User practices and potential threats. In *2017 IEEE European symposium on security and privacy (EuroS&P)*, pages 417–432. IEEE, 2017.

[18] Luuk Hendriks, Ricardo de Oliveira Schmidt, Roland van Rijswijk-Deij, and Aiko Pras. On the potential of ipv6 open resolvers for ddos attacks. In *International Conference on Passive and Active Network Measurement*, pages 17–29. Springer, 2017.

[19] NP. Hoang, AA. Niaki, J. Dalek, J. Knockel, P. Lin, B. Marczak, M. Crete-Nishihata, P. Gill, and M. Polychronakis. How Great is the Great Firewall? Measuring China's DNS Censorship. In *30th USENIX Security Symposium*, pages 3381–3398. USENIX Association, 2021.

[20] Geoff Huston. IPv6 in 2020. https://blog.apnic.net/2021/02/08/ipv6-in-2020/. Accessed: 2022-01-25.

[21] Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. Ethical concerns for censorship measurement. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*, NS Ethics '15, page 17–19, New York, NY, USA, 2015. Association for Computing Machinery.

[22] Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, and Thorsten Holz. Going wild: Large-scale classification of open dns resolvers. In *Proceedings of the 2015 Internet Measurement Conference*, pages 355–368, 2015.

[23] Solomon Kullback and Richard A Leibler. On information and sufficiency. *The annals of mathematical statistics*, 22(1):79–86, 1951.

[24] Citizen Lab and Others. Url testing lists intended for discovering website censorship, 2014. https://github.com/citizenlab/test-lists.

[25] Philip Levis. The collateral damage of internet censorship by dns injection. *ACM SIGCOMM CCR*, 42(3):10–1145, 2012.

[26] Graham Lowe, Patrick Winters, and Michael L Marcus. The great dns wall of china. *MS, New York University*, 21:1, 2007.

[27] P. Mockapetris. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION . *Internet Engineering Task Force*, 1987. Accessed: 2022-01-27.

[28] Austin Murdock, Frank Li, Paul Bramsen, Zakir Durumeric, and Vern Paxson. Target generation for internet-wide ipv6 scanning. In *Proceedings of the 2017 Internet Measurement Conference*, pages 242–253, 2017.

[29] Zubair Nabi. The anatomy of web censorship in pakistan. In *3rd {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 13)*, 2013.

[30] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. Iclab: A global, longitudinal internet censorship measurement platform. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 135–151. IEEE, 2020.

[31] Ramakrishna Padmanabhan, Arturo Filastò, Maria Xynou, Ram Sundara Raman, Kennedy Middleton, Mingwei Zhang, Doug Madory, Molly Roberts, and Alberto Dainotti. A multi-perspective view of internet censorship in myanmar. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet*, pages 27–36, 2021.

[32] Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson. Augur: Internet-wide detection of connectivity disruptions. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 427–443. IEEE, 2017.

[33] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. Global measurement of {DNS} manipulation. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 307–323, 2017.

[34] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. Decentralized control: A case study of russia. In *Network and Distributed Systems Security (NDSS) Symposium 2020*, 2020.

[35] Will Scott, Thomas Anderson, Tadayoshi Kohno, and Arvind Krishnamurthy. Satellite: Joint analysis of cdns and network-level interference. In *2016 {USENIX} Annual Technical Conference ({USENIX}{ATC} 16)*, pages 195–208, 2016.

[36] Ryan Shandler. Measuring the political and social implications of government-initiated cyber shutdowns. In *8th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 18)*, 2018.

[37] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. Censored planet: An internet-wide, longitudinal censorship observatory. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 49–66, 2020.

[38] S. Thomson, C. Huitema, Ksinant V., and Souissi M. DNS Extensions to Support IP Version 6 . *Internet Engineering Task Force*, 2003. Accessed: 2022-01-27.

[39] Benjamin VanderSloot, Allison McDonald, Will Scott, J Alex Halderman, and Roya Ensafi. Quack: Scalable remote measurement of application-layer censorship. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pages 187–202, 2018.

[40] Matthäus Wander, Christopher Boelmann, Lorenz Schwittmann, and Torben Weis. Measurement of globally visible dns injection. *IEEE Access*, 2:526–536, 2014.

[41] Zachary Weinberg, Diogo Barradas, and Nicolas Christin. Chinese wall or swiss cheese? keyword filtering in the great firewall of china. In *Proceedings of the Web Conference 2021*, pages 472–483, 2021.

[42] Xueyang Xu, Z Morley Mao, and J Alex Halderman. Internet censorship in china: Where does the filtering occur? In *International Conference on Passive and Active Network Measurement*, pages 133–142. Springer, 2011.

[43] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. Where the light gets in: Analyzing web censorship mechanisms in india. In *Proceedings of the Internet Measurement Conference 2018*, pages 252–264, 2018.

A Full list of countries / resolvers

Country	Resolver	IPv4	IPv4	IPv6	IPv6	Avg.
	pairs	A	AAAA	A	AAAA	
United States (US)	1228	1.40	0.94	0.49	0.85	0.92
Germany (DE)	753	1.00	0.92	0.75	0.81	0.87
Korea (KR)	632	2.33	1.06	1.24	1.22	1.46
France (FR)	560	0.56	0.47	0.39	0.54	0.49
Russia (RU)	312	5.51	4.78	4.49	4.50	4.82
Iran (IR)	277	25.12	24.49	21.95	21.45	23.25
Viet Nam (VN)	252	1.53	0.89	1.42	0.67	1.13
Taiwan (TW)	248	1.16	1.03	0.86	0.95	1.00
India (IN)	226	1.27	1.52	1.04	1.16	1.25
Canada (CA)	199	0.74	0.36	0.23	0.30	0.41
United Kingdom (GB)	196	1.14	0.92	0.77	0.97	0.95
China (CN)	194	29.27	32.32	28.41	32.08	30.52
Thailand (TH)	186	8.25	1.18	1.13	0.93	2.87
Brazil (BR)	160	2.67	1.67	1.99	2.08	2.10
Japan (JP)	152	1.12	1.18	0.56	1.01	0.97
Mexico (MX)	150	3.78	2.05	1.75	1.94	2.38
Turkey (TR)	114	1.29	0.96	1.27	1.02	1.14
Netherlands (NL)	97	1.17	0.78	0.72	0.70	0.85
South Africa (ZA)	93	2.41	1.60	1.18	1.33	1.63
Australia (AU)	72	1.56	0.70	0.95	0.66	0.97
Hong Kong (HK)	67	7.00	5.57	4.91	5.24	5.68
Chile (CL)	65	2.67	0.70	1.10	0.79	1.32
Switzerland (CH)	60	0.32	0.34	0.28	0.34	0.32
Indonesia (ID)	56	6.46	2.99	2.41	2.26	3.53
Lithuania (LT)	52	0.95	0.80	0.51	0.78	0.76
Singapore (SG)	50	1.76	0.86	0.64	0.78	1.01
Malaysia (MY)	50	4.92	2.03	1.27	1.35	2.39
Spain (ES)	49	0.91	0.75	1.40	1.94	1.25
Poland (PL)	48	2.00	1.13	2.90	0.96	1.75
Argentina (AR)	47	5.20	3.51	2.22	1.28	3.05
Romania (RO)	44	2.30	1.03	0.83	0.93	1.27
Czechia (CZ)	41	1.60	1.06	0.50	0.51	0.91
Italy (IT)	38	2.36	2.10	2.25	2.52	2.31
Ukraine (UA)	35	6.49	3.05	2.64	2.87	3.76
Sweden (SE)	34	0.36	0.29	0.51	0.25	0.35
Finland (FI)	34	0.68	0.59	0.43	0.52	0.56
Belgium (BE)	31	1.56	1.26	0.95	0.95	1.18
Bulgaria (BG)	30	3.24	2.91	1.15	1.06	2.09
Bangladesh (BD)	29	6.42	1.28	0.89	0.81	2.35
Colombia (CO)	27	3.39	3.28	1.45	1.14	2.31
Saudi Arabia (SA)	24	2.21	1.81	1.60	1.60	1.81
Pakistan (PK)	23	3.74	1.59	4.64	1.86	2.96
Hungary (HU)	22	0.29	0.27	0.23	0.31	0.27
Ecuador (EC)	21	3.29	2.94	0.38	0.77	1.84
Greece (GR)	20	0.49	1.15	0.41	0.53	0.64
Kazakhstan (KZ)	19	2.90	2.01	2.42	2.21	2.38
Philippines (PH)	18	4.34	2.36	2.45	1.96	2.78
Norway (NO)	16	0.27	0.32	0.31	0.40	0.32
Slovakia (SK)	14	0.22	0.24	0.22	0.26	0.24
Egypt (EG)	14	5.59	4.12	3.05	3.47	4.06
Denmark (DK)	13	1.68	1.26	0.93	1.05	1.23
Portugal (PT)	11	2.16	0.39	0.23	0.27	0.76
Peru (PE)	11	2.04	0.81	0.69	0.65	1.05
Nigeria (NG)	9	3.42	1.38	1.65	1.43	1.97
Austria (AT)	8	0.11	0.19	0.07	0.14	0.13
Kenya (KE)	8	7.79	1.40	1.14	1.07	2.85
Moldova, Republic of (MD)	7	5.46	3.58	2.90	3.04	3.75
Serbia (RS)	7	0.18	0.12	0.14	0.10	0.14
Nepal (NP)	7	1.10	1.22	0.80	0.98	1.03
Slovenia (SI)	7	3.48	0.24	0.14	0.16	1.01
New Zealand (NZ)	7	4.30	0.20	0.46	0.16	1.28
United Arab Emirates (AE)	6	1.61	0.86	1.10	0.89	1.11
Estonia (EE)	6	1.61	0.42	0.28	0.42	0.68
Costa Rica (CR)	6	8.57	2.45	2.19	2.10	3.83
Uruguay (UY)	6	0.70	0.42	0.23	0.19	0.39
Macao (MO)	6	4.44	4.48	4.44	4.51	4.46
Mongolia (MN)	5	1.88	0.67	0.59	0.70	0.96
Libya (LY)	5	1.40	0.76	0.39	0.42	0.74
Sudan (SD)	5	4.59	4.48	2.38	2.32	3.45

Venezuela (VE)	5	6.67	1.62	0.81	0.73	2.46
Belarus (BY)	5	1.01	0.73	0.45	0.62	0.70
Panama (PA)	5	3.75	3.98	0.31	0.45	2.12
Armenia (AM)	5	0.87	0.64	0.59	0.73	0.71
Uzbekistan (UZ)	4	0.53	0.85	0.82	0.74	0.74
Belize (BZ)	4	5.92	0.53	0.42	0.39	1.81
Latvia (LV)	4	0.11	0.11	0.14	0.14	0.12
Luxembourg (LU)	4	1.86	0.07	0.07	0.21	0.55
Albania (AL)	4	0.70	0.56	0.42	0.42	0.53
Iraq (IQ)	4	3.57	2.45	2.14	2.14	2.57
Bosnia and Herzegovina (BA)	4	2.21	0.70	0.63	0.70	1.06
Guatemala (GT)	4	0.60	0.56	0.39	0.21	0.44
Jordan (JO)	4	0.28	0.21	0.14	0.42	0.26
Bolivia (BO)	4	1.16	0.53	0.32	0.28	0.57
Lebanon (LB)	3	0.61	0.33	0.28	0.33	0.39
Dominican Republic (DO)	3	4.76	0.75	0.28	0.47	1.56
Honduras (HN)	3	1.49	1.45	0.65	0.61	1.05
Croatia (HR)	3	0.14	0.23	0.19	0.14	0.18
Afghanistan (AF)	3	2.24	1.12	1.91	1.82	1.77
Cambodia (KH)	3	3.17	0.90	0.47	0.43	1.24
El Salvador (SV)	2	0.84	0.35	0.14	0.21	0.39
Nicaragua (NI)	2	3.78	0.28	0.35	0.07	1.12
Lao (LA)	2	9.24	0.56	0.21	0.28	2.57
Oman (OM)	2	5.46	0.70	0.42	0.70	1.82
Israel (IL)	2	2.73	2.94	2.73	2.66	2.77
Guam (GU)	2	8.05	0.35	0.00	0.35	2.19
Georgia (GE)	2	1.19	1.26	1.40	0.98	1.21
Trinidad and Tobago (TT)	2	0.35	0.14	0.07	0.00	0.14
Chad (TD)	2	2.73	1.05	0.63	1.12	1.38
North Macedonia (MK)	2	9.52	6.44	4.69	4.83	6.37
Ethiopia (ET)	2	0.14	0.28	25.56	0.21	6.55
Uganda (UG)	2	0.49	0.49	0.56	6.65	2.05
Tunisia (TN)	2	0.35	0.42	0.35	0.49	0.40
Cyprus (CY)	2	4.83	0.70	0.35	0.21	1.52
Paraguay (PY)	1	3.26	1.56	1.28	1.13	1.81
Kyrgyzstan (KG)	1	0.57	0.71	0.43	0.85	0.64
Seychelles (SC)	1	0.28	0.43	0.28	0.57	0.39
Global	7,428	3.10	1.83	1.77	1.60	2.07

Table 7: Full list of measured rates of DNS censorship across both query types and network interfaces. Rates are expressed as the percentage of censored DNS queries over total number of DNS queries sent. Darker shaded cells indicate a higher rate of DNS censorship (compared to the country's average) and lighter shaded cells indicate a lower rate of DNS censorship. The average rate of censorship for a country is computed across all four IP/query combinations. The global row contains the mean of each column. These means weigh the contribution of each country equally, rather than weighted by the number of resolvers used in tests.