Efficacy and Collateral Damage of Censorship: A Case-Study of Austria Blocking Cloudflare

Tobias Fiebig
MPI for Informatics
tfiebig@mpi-inf.mpg.de

Martina Lindorfer
TU Wien
martina.lindorfer@tuwien.ac.at

Carlos H. Gañán
TU Delft
C.HernandezGanan@tudelft.nl

Oliver Gasser
MPI for Informatics
oliver.gasser@mpi-inf.mpg.de

ABSTRACT

Between the 28^{th} and 29^{th} of August 2022 a digital rights holder organization in Austria requested 11 IP addresses used by Cloudflare's anycast CDN to be blocked by Austrian ISPs in an attempt to block two websites distributing copyrighted material. Over the evening of the 28^{th}, this was implemented by several ISPs, leading to connectivity issues for other sites using Cloudflare that were also using these addresses. In this paper, we analyze this incident, describe its timeline, and assess the order of magnitude of affected sites using a passive DNS dataset. Besides assessing the collateral damage, we also analyze the theoretical efficacy of the censorship attempts given the prevalence of multiple IPv4 addresses as well as IPv6 being used for sites behind a CDN. We find that the censorship attempts had substantial collateral damage in the tenth of thousands of sites, while their efficacy was limited.

CCS CONCEPTS

• **Social and professional topics** → **Censoring filters**; **Technology and censorship**; **Network access restrictions**; *Internet governance / domain names*; *Secondary liability*;

KEYWORDS

Censorship Measurements, CDN, Content Blocking

1 INTRODUCTION

Internet censorship is a pervasive issue around the globe [79]. While, from a global-north perspective, the common censorship example is the 'Chinese Great Firewall' [4, 86], several states in the global north have already deployed infrastructure to 'block' unwanted websites and content for constituents in their jurisdiction [23]. The reasoning behind deploying this kind of infrastructure varies, and ranges from combating Child Sexual Abuse Material (CSAM) [52], over preventing illegal gambling [12] and the enforcement of sanctions [23], to preventing copyright infringement [56]. Especially the latter point currently sees efforts from European policy makers to undermine central security and privacy features to ensure copyrighted material is not illicitly uploaded [57].

While, especially in Europe, platforms for censorship were often built on Domain Name System (DNS) blocking, which can easily be circumvented, the trend moves towards infrastructure that also allows blocking based on IP addresses. This point has been further underlined by efforts for 'bottom-up sanctions' by the Internet community [85] to use blackholing [28] to enable voluntary sanctions against individual addresses by network operators.

As with all large-scale tooling, censorship infrastructure has a tendency to over-block and cause false positives. With the bottom-up sanctions of the networking community, voluntary participation succumbed to the tiered nature of the Internet [23]. Similarly, censorship infrastructure used for content moderation regularly receives attention for false positives, severely impacting the life of those affected. Network blocking is, of course, not exempt from these issues, and faced criticism for overblocking in the past [8].

On the 28^{th} of August 2022, a block request for 14 domains of two services and 11 IPv4 addresses from the Austrian copyright collecting company *LSG – Wahrnehmung von Leistungsschutzrechten GesmbH* was submitted to Austrian Internet Service Providers (ISPs), instructing them to prevent their customers from accessing them [21, 49]. However, as the IP addresses for which blocking was requested are part of Cloudflare's Global Service Load Balancer (GSLB) setup, several other sites were affected as well. This naturally raises the question: *how many sites were a collateral in this censorship attempt?*

In this paper, we make the following contributions:

Censorship efficacy: We document the timeline and impact on initially targeted sites, assessing the efficacy of the censorship mechanic.

Affected websites: We estimate a lower and upper bound for the individual sites affected by this incident, finding between 63,126 and up to 277,834 unique impacted domains.

Popularity and protected entities: We analyze the popularity of affected domains and investigate case-studies of noteworthy affected websites, highlighting how this incident affected sites of protected entities, stretching into serious social consequences, such as freedom of the press or freedom of religion.

Structure: In Section 2, we provide a brief summary of censorship infrastructure and associated technology, as well as a detailed timeline of the incident we investigate in this paper. We then describe our dataset in Section 3, before presenting our results and case-studies in Section 4. Finally, we reflect on our findings in Section 5, before concluding in Section 6.

2 BACKGROUND

In this section, we first provide an overview of different technical measures to prevent content from being accessed, as well as contextualizing related research on Internet censorship. Next, we discuss CDN mechanics, before describing the case we investigate in this paper.

2.1 Censorship Methods

Censorship infrastructure commonly works on one or multiple levels [30]: i) preventing service discovery, ii) preventing connectivity to services, iii) content inspection. In addition, if local laws and laws in the hosting region align, authorities can also attempt to have the content removed from the hosting systems.

Preventing Service Discovery: Due to DNS being unsigned and unencrypted before DNSSEC [5] and DoT/DoH/DoQ [33, 36, 37], suppressing or changing DNS responses for sites supposed to be censored was one of the earliest approaches to censorship [41]. DNS blocking relies on the cooperation of the users' recursive DNS resolver in the censorship attempt. Furthermore, DNS blocking is employed by users and organizations to limit tracking on the Internet [75], implement youth protection [42], and to combat malware [58].

Technically, DNS blocks via recursive resolvers can be easily circumvented, if users run their own recursive DNS resolver, or switch to a non-censoring DNS provider [41]. Especially the latter became prevalent with the rise of the 'non-lying quad DNS resolvers', i.e., `1.1.1.1` (Cloudflare), `8.8.8.8` (Google), and `9.9.9.9` (IBM/PCH). To combat this, network operators can block or redirect users' DNS requests. This, in turn, was one of the motivating issues for developing and deploying DoH [33].

Preventing Connectivity: The next level of censorship infrastructure attempts to directly prevent connectivity to sites on the IP layer. This, in essence, is comparable to firewalling in most cases. An ISP is instructed to block all requests from their users for specific IP addresses. The challenge here is to identify relevant IP addresses. Addresses can be changed by censored sites with relative ease, and due to virtual hosts and Server Name Indication (SNI) [20] multiple services may run on a single IP address, making it challenging to not overblock. At the same time, identifying an IP address of a target site can also become a challenge if the site hides behind a Content Delivery Network (CDN), as is commonly necessary to thwart distributed denial-of-service (DDoS) attacks [23]. Moreoever, identifying the right block granularity is challenging for IPv6 addresses [60]. In addition, IP blackholing [28] can be used to distribute blocked addresses to network operators, a proposal also discussed in 2022 in the wake of Russia's war against Ukraine [23, 85]. Similarly, various entities called for Internet number authorities (Regional Internet Registries and ICANN) to revoke assigned IP addresses and domain names for various reasons [6, 73].

Content Inspection: The 'gold standard' of censorship systems are setups that employ Deep Packet Inspection (DPI) to make blocking decisions based on the transferred content. The canonical example for such a system is the 'Great Firewall of China' (GFW), which intercepts packets on multiple layers and combines static blocking with content-specific actions [87], for example based on keywords [3, 14]. A major challenge for most DPI-based censorship solutions is the rise of encrypted traffic [27]. This lead to the development and deployment of approaches to enable DPI despite encryption [19, 31, 74] or limit the use of encryption in general [40]. DPI middleboxes [16, 43, 45] are nowadays used in enterprise networks to monitor and mitigate threats to the network [55], identify the illicit extraction of information [80], and ensure corporate policy on Internet use [47]. One major challenge of moving these systems from a corporate environment to a censorship system for the general population—comparable to the GFW—is scaling to the traffic volumes experienced on Internet links [13].

In comparison to previously described censorship technologies, accuracy for DPI-based solutions can be higher, as they can, for example, evaluate SNI headers to only block specific virtual hosts. Nevertheless, especially when focusing on *specific* content and not whole sites, DPI solutions also require attacks on end-to-end encryption, to enable the inspection of encrypted packets. Hence, even though they may reduce overblocking, they also require a substantially stronger violation of users' rights to be deployable. Techniques such as the TLS Encrypted Client Hello [59] could further increase the hurdles for DPI blocking by hiding the domain name in the handshake, should they see widespread deployment in the future [29, 39, 54].

Examples from Related Work: Research on various forms of content blocking and censorship is pervasive. For example, McDonald et al. [51] measure CDN's geo-blocking, often related to local policies on permissible content. Sundara Raman et al. [78] take a more comprehensive approach, building a global censorship observatory. Related, VanderSloot et al. [82] introduce a technique to remotely measure application-layer censorship, and Bock et al. [11] investigate HTTPS censorship techniques in China. Tangentially, researchers have also studied censorship evasion techniques [10], and how to better detect them at scale [32]. Finally, Bock et al. [9] also explored offensive techniques to utilize censorship infrastructure for denial-of-service attacks.

Table 1: Overview of domains and IPv4 addresses that the *LSG – Wahrnehmung von Leistungsschutzrechten GesmbH* requested to be blocked by Austrian ISPs.

Idx.	Domain
1	newalbumreleases.net
2	newalbumreleases.unblockit.bet
3	newalbumreleases.unblockit.ist
4	newalbumreleases.unblockit.buzz
5	newalbumreleases.unblockit.ch
6	newalbumreleases.unblockit.club
7	newalbumreleases.unblockit.li
8	newalbumreleases.unblockit.link
9	newalbumreleases.unblockit.onl
10	newalbumreleases.unblocked.co
11	newalbumreleases.unblockit.uno
12	canna-power.to
13	canna.to
14	uu.canna.to

Idx.	IP Address
1	104.31.16.119
2	104.26.12.95
3	172.67.175.231
4	188.114.97.12
5	104.21.88.201
6	188.114.96.12
7	104.21.69.123
8	104.21.6.167
9	104.21.36.27
10	46.148.26.245
11	46.148.26.194

2.2 Load Balancing & Anycast-based CDNs

Cloudflare operates a CDN and DDoS prevention service with global operations. The CDN product of Cloudflare uses Global Service Load Balancers (GSLBs) [15] located in anycast networks around the globe [15] to serve customers' traffic. Customers' content can either be hosted on Cloudflare systems directly, or on application servers for which Cloudflare only acts as the load balancer/frontend. While anycast is the major traffic handling tool for Cloudflare, low Time-To-Lives (TTLs) of 300 seconds on DNS records would also enable traffic shifting by returning specific DNS records to clients, e.g., facilitated by the EDNS Client Subnet extension [77], to direct clients to specific anycast nodes. This, however, is not the main technique used by Cloudflare.

2.3 Case Description

Internet censorship in Austria is regulated in §81 Abs. 1a UrhG ('Urheberrechtsgesetz,' i.e., copyright law) [7]. This law specifies that copyright holders can submit a petition to be granted by a judge to have specific URIs and IP addresses blocked. URIs and IP addresses for which a petition is granted are communicated to ISPs, which then have to implement technical measures ensuring these sites are not reachable by their customers. Following the chain of events outlined below, it is likely that ISPs use DNS blocks when they have to censor domain names, while using blackholing when specific IP addresses are supplied.

On the 28^{th} of August 2022, a petition to block 14 domains of two services and 11 IPv4 addresses from the Austrian copyright collecting company *LSG – Wahrnehmung von Leistungsschutzrechten GesmbH*, effective 29^{th} of August 2022, was added to this list [49], see Table 1. These 11 IPv4 addresses are in use by Cloudflare on their GSLB to make customers' websites accessible.

At 16:30 UTC on 28^{th} of August 2022 a post was started on the HackerNews forum, noting that Austrian ISPs were ordered to block IPs in use by Cloudflare [84]. The thread quickly expanded and several users reported connectivity issues.

Over the next hours, users of Austrian ISPs experienced connectivity issues, until Cloudflare took action [76]—not pointing to affected addresses for users of blocking ISPs—and ultimately the block was lifted on the 29^{th} of August 2022. The ISPs that implemented the block on the IP level were, according to RIPE Atlas data collected from 21:45 UTC on the 28^{th} onward every 10 minutes [62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72], Salzburg AG, Magenta, and A1, see Figure 1. The blocks were lifted the next day, around 10:00 UTC (Magenta), 12:45 UTC (A1), and 14:45 (Salzburg AG). Furthermore, as seen in Figure 2, parts of A1 also implemented blocking based on TLS handshakes, as TLS handshakes to a specific affected site were not possible, despite the site being reachable via ICMP. These blocks for A1 persisted even longer, stretching up until 16:45 UTC on the 29^{th} of August 2022.

3 DATASET & METHODOLOGY

In this section, we introduce the Farsight SIE dataset [22], with which we measure the impact of the Austrian censorship attempts, summarize our methodology, and discuss limitations and ethics.

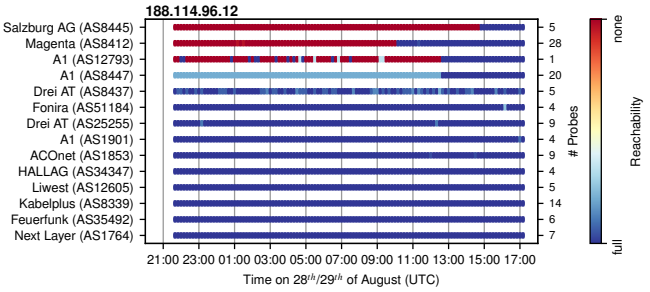


Figure 1: Overview of ICMP reachability for 188.144.96.12 on 28^{th}/29^{th} of August 2022 from RIPE Atlas probes [62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72] in Austrian ISPs.

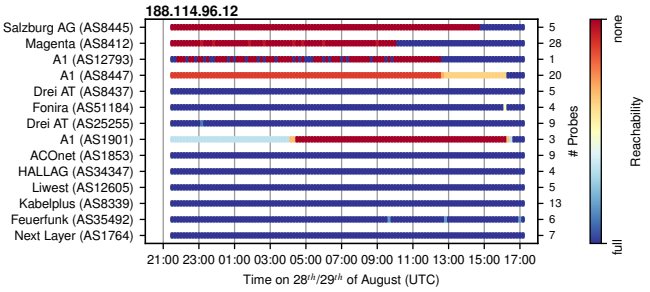


Figure 2: Overview of reachability via TLS on TCP/443 for 188.144.96.12 during 28^{th}/29^{th} of August 2022 from major Austrian ISPs based on RIPE Atlas data [61].

3.1 Dataset Description

To measure which names pointed to IP addresses affected by the censorship attempts, we utilize Farsight data for each day in August 2022. The Farsight dataset is collected from major recursive DNS resolvers around the world. To prevent the collection of personally identifiable information, Farsight only collects DNS 'cache misses.' Cache misses occur when a recursive DNS resolver has to query the DNS for a requested name, because it does not have a version of that name that is younger than the record's TTL in its local cache. For business confidentiality reasons, Farsight does not share the exact number and location of its sensors. Still, the efficacy, coverage, and applicability for research of the Farsight dataset have been demonstrated in the past [26], and it is regularly used in measurement studies [24, 35, 48]. The Farsight dataset is more suitable for our research question than, e.g., active datasets like the OpenINTEL dataset [34, 81, 83], as Farsight sensors are globally distributed, and therefore the impact of vantage-point location in the context of DNS and CDN measurements [77] is reduced, see also Section 3.3.

Over the month of August our dataset contains 5.5B unique requested names, including 3.2B names with resource record type (RRtype) `A` (mapping names to IPv4 addresses), 1.1B with RRtype `AAAA` (mapping names to IPv6 addresses), and 0.4B with RRtype `NS` (identifying authoritative DNS servers for a zone), see Figure 3 for an overview per day. For a comprehensive summary of DNS related terminology, please see Appendix A.2 of Fiebig et al. [25].

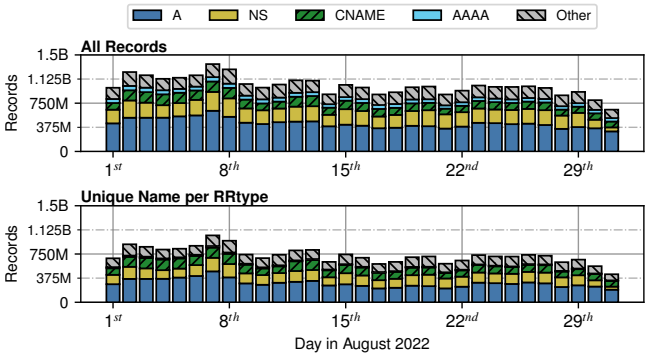


Figure 3: Overview of unique names per RRtype in the raw dataset for August 2022.

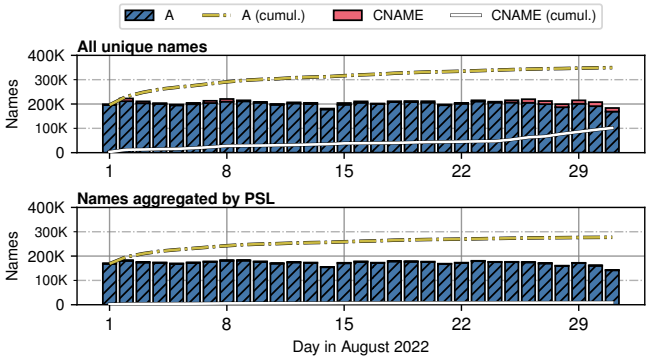


Figure 4: Names associated with the IP addresses from Table 1 at some point in time during August 2022.

3.2 Data Extraction & Augmentation

To extract all relevant names from the dataset, we first obtained all names whose A records pointed to at least one of the IP addresses included in the block request for each day in August 2022, see Table 1. We then identify the private suffix, i.e., domain of each of those names using the Mozilla Public Suffix List [53] and extract all entries from the dataset who fall under the same private suffix, regardless of the IP address they point to at that time, as well as all CNAMEs[1] pointing to these names.

This process yielded 349,469 unique names with RRtype A and 101,512 unique CNAMEs. Aggregating this data using the Mozilla Public Suffix List [53], we see 277,129 unique names with RRtype A and 8,928 unique CNAMEs, leading to 280,272 unique private suffixes due to an overlap between these two groups. See Figure 4 for an overview of unique names per day.

For our further analysis, also given limitations below, we aggregate our inputs to a monthly perspective. In this process, we consider a tuple of requested name, RRtype, and response to occur at the whole timeframe between its first and last observation. Furthermore, we resolve all CNAMEs to the respective IP addresses to which they ultimately point, i.e., look up the A/AAAA records of the names they point to from the passive dataset. We then conduct our analysis on these aggregated timeframes.

3.3 Dataset Limitations

The Farsight dataset has several limitations which we have to consider when interpreting our results. Specifically:

Visibility: The dataset only contains requests and responses for which a cache miss occurred behind one of Farsight's sensors. Hence, we only see domains that have been actively queried during the measurement period. In turn, this means that our visibility is reduced especially for less popular sites. To address this, we perform the aforementioned aggregation, and acknowledge that our results can only provide a lower bound.

Vantage Point: The location of querying clients is an important aspect of DNS measurements, especially as various operators deliver different DNS responses to clients based on their location, e.g., for traffic steering [77]. Hence, names we find to return addresses affected by the Austrian censorship activities *might* have returned different names when requested by clients in the blocking ISPs. This limitation means that our lower bound estimates correspond to *potentially* affected sites. Nevertheless, given that Cloudflare is an anycast based CDN and does not use DNS for load balancing, and the wide global spread of sensors, we consider this to have limited impact on our estimation of a *lower bound*.

Hence, despite these limitations, we consider our methodology appropriate to illustrate our research questions, and highlight the collateral damage censorship attempts can have.

3.4 Ethical Considerations

In this work we use the Farsight SIE dataset [22], which collects DNS data from various globally-distributed sensors. These sensors only collect cache misses beyond the recursive resolver, which ensures that personal identifiable information (PII) of Farsight's clients is protected. We handle the Farsight dataset according to best measurement practices [1, 44].

4 MEASUREMENT RESULTS

In this section, we present our observations on affected sites based on the Farsight dataset. We first summarize the overall number of potentially affected domains, and then analyze how these spread over different top-level domains (TLDs) and popularity.

4.1 Overview of Affected Sites

To get a reliable lower bound of affected domains, we investigate names for which we observed requests between 28^{th} 16:00 UTC and 29^{th} 17:00 UTC of August 2022, the time during which blocks were in place by at least some ISPs. Figure 5 depicts an overview of that part of our dataset with hourly granularity from the 28^{th} 00:00 UTC to the 30^{th} 00:00 UTC. Each bar represents the names during that hour for which we saw a) only blocked A/IPv4 records (Only Matching), b) only blocked A/IPv4 records, but also completely unblocked AAAA/IPv6 records (Only Matching+AAAA), c) blocked and unblocked A/IPv4 records (Matching), and d) blocked and unblocked A/IPv4 records plus completely unblocked AAAA/IPv6

[1] CNAMEs are DNS records that allow pointing from one DNS entry to another for the answer, see Fiebig et al. [25].

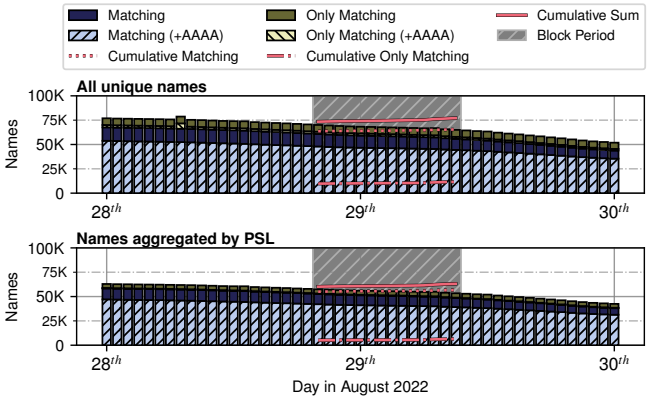
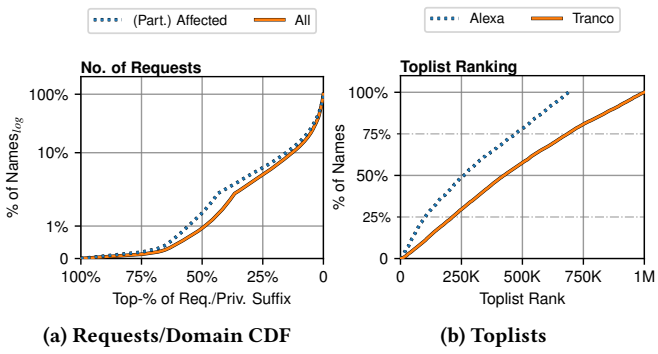


Figure 5: Overview of names returning IP addresses from Table 1 during the block period between 28^{th} 16:00 UTC and 29^{th} 08:00 UTC of August 2022.



(a) Requests/Domain CDF **(b) Toplists**

Figure 6: Overview of the number of requests observed for all observed domains and (partially) affected domains (Figure 6a) and affected sites ranked by the Alexa and Tranco top lists (Figure 6b). The popularity of sites is evenly distributed across all affected sites, i.e., few highly popular sites, while the large body of sites is less popular. The distribution of affected sites in terms of requests is similar to that of all sites.

records (Matching+AAAA). When we now investigate the cumulative sum—assuming that DNS records retained their IP addresses even if we did not observe them during all hours of the blocking period—we find 77,093 unique names (63,126 private suffixes) pointing to at least one blocked IP address. Of those, 65,463 unique names (56,713 private suffixes) also return at least one unblocked IP address. Looking at IPv6, from the 77,093 unique names (63,126 private suffixes) a total of 54,039 (45,899 private suffixes) also returned at least one IPv6 address in this period.

Hence, in summary, we find that the attempted censorship of effectively two specific sites caused collateral damage to *at least* 63k sites, making them partially unreachable or increasing connection times during the block period. Additionally, 5.6k sites were completely affected as all IPv4 addresses their DNS records pointed to were blocked, and an additional 0.8k sites were only reachable for IPv6 enabled clients via their IPv6 addresses, as all IPv4 addresses their records point to were blocked. However, given the partial perspective of the Farsight dataset, this can only be a lower bound.

4.2 Affected TLDs

To get a better perspective of blocked domains, we also investigated how (partially) affected private suffixes distribute over different TLDs, see Table 2. We find that the distribution is similar for private suffixes, independent of them having associated `AAAA` records. Furthermore, in general, the distribution roughly corresponds to the popularity ranking provided by ICANN [38], where ICANN ranks the popularity of certain domains based on their prevalence at the DNS root servers. This, of course, excludes expected exceptions like `.arpa`, as it is an infrastructure domain. Similarly, `.xyz` is more commonly found in the dataset of affected domains than in the ICANN ranking. Nevertheless, we obtain a picture where domains affected by the blocks seem to be reasonably evenly distributed over the general domain population.

4.3 Popularity of Affected Sites

Next, we analyze the popularity of affected sites using cache miss volume and toplists. We first investigate the number of cache misses observed for each site's `CNAME` and `A` RRs during our measurement period. Usually, the number of cache misses in the Farsight dataset is not a useful metric for the popularity of sites, as the TTL of the associated records is not included in the dataset [25]. However, in this instance, we are dealing with DNS records served from Cloudflare's authoritative name server, ensuring a relative homogeneity of TTLs, as the default TTL value for records served by Cloudflare's anycast infrastructure is 300 seconds [17]. Plotting the cumulative counts for all domains (private suffixes) pointing to at least one affected record, we see a normal heavy-tail distribution, see Figure 6a, while the distribution of requests does not differ when comparing all encountered names during the period with only those affected by the block. Put more colloquially, we find that affected sites range from a large body of less popular sites to a variety of sites receiving a high number of requests.

To confirm this observation independently, we also rank the affected sites in our sample using the latest Alexa Top List [2] as well as the Tranco Top 1M [46], see Figure 6b. While both top lists naturally only cover a fraction of our sites—the most popular ones—we find that for those most popular sites the distribution over toplist ranks is evenly spaced. Hence, our comparison to toplists further supports our finding that sites of all popularity levels have been affected by the blocking attempts observed in Austria. In general, this aligns with our observation of sites from a wide variety of TLDs having been affected, again hinting at an evenly distributed and random sample of different domains among Cloudflare's customer base having been affected.

5 DISCUSSION

In this section, we discuss the efficacy of the observed censorship attempts and their impact on society.

5.1 Efficacy of Blocking

Revisiting the domains and IP addresses from Table 1, we find that all explicitly blocked domain names have at least one IP address

Table 2: Overview of distribution of affected TLDs across public suffixes. For comparison, we list the TLD ranking Top 10 from ICANN's view on authoritative servers, collected on the 6^{th} of October 2022. [38].

IPv4 & IPv6			IPv4 Only			Sum			ICANN Statistics		
Rank	TLD	Count	Rank	TLD	Count	Rank	TLD	Count	Rank	TLD	Volume
1	.com	22,400	1	.com	7,721	1	.com	30,121	1	.com	1,300M
2	.net	2,286	2	.org	1,104	2	.org	3,136	2	.net	619M
3	.org	2,032	3	.co.uk	872	3	.net	3,096	3	.org	92M
4	.de	1,599	4	.net	810	4	.co.uk	1,936	4	.arpa	153M
5	.xyz	1,225	5	.co.za	504	5	.de	1,809	5	.info	34M
6	.ru	1,176	6	.tk	328	6	.ru	1,335	6	.uk	36M
7	.co.uk	1,064	7	.ca	279	7	.xyz	1,313	7	.biz	16M
8	.io	382	8	.com.au	262	8	.co.za	851	8	.io	26M
9	.top	373	9	.de	210	9	.com.au	630	9	.de	21M
10	.com.au	368	10	.in	200	10	.ca	576	10	.eu	12M
	Other:	12,994		Other:	4,760		Other:	18,323			
Total:		45,899	**Total:**		17,227	**Total:**		63,126			

that has been blocked as well associated with them in the dataset. Note that two explicitly blocked names are not in the dataset. However, we find at least one additional unblocked IP address associated with each explicitly blocked name. While this might be due to DNS responses from other regions (see Section 3.3), it also means that restoring functionality for the CDN operator would have been as easy as returning those unblocked addresses for Austrian users. Similarly, out of the 14 blocked domains in the dataset, all but domains related to `newalbumreleases.net` and `canna.to` have associated IPv6 addresses, which were not blocked at all.

Furthermore, we also find 16 additional names following the pattern around `newalbumreleases.net`, and two additional domains around `canna.to` not contained in the blocklist. For the former, each of these names shows up with blocked and unblocked IP addresses in the dataset. For `canna.to`, the operator claims on their site that the addition of new domains was a direct response to earlier block attempts in Austria[2]. Hence, in summary, we find that—despite their substantial collateral damage—the censorship attempts did not completely cover the content supposed to be blocked. This also aligns with actions of Internet blocking by nation states, who—if pressed to—many times do not try to selectively censor the Internet, but rather attempt to turn it off all together [18, 50].

Looking at the wider population of 77,093 unique names that were at least partially affected (63,126 private suffixes), we find that 65,463 (56,713 private suffixes) of them—84.9%/89.8%, respectively—also have at least one non-affected IPv4 address associated with them. When we expand this perspective to IPv6, we find that of the 77,093 unique names at least partially affected (63,126 private suffixes), 54,039 (45,899 private suffixes)—70.1%/72.7%, respectively—also have at least one IPv6 address associated with them, which were not impacted at all. A total of 2,761 unique names and 804 private suffixes furthermore had an IPv6 address associated with them while all associated IPv4 addresses were affected by the censorship attempts. Given that, from the ISPs that actively blocked affected sites, only Salzburg AG does not implement IPv6 for its end users, this further reduces the efficacy of the blocking attempt, as users could still access the blocked content over IPv6.

[2]https://web.archive.org/web/20220901082130/https://canna-power.to/

5.2 Censorship & Society

Following our results, the censorship attempts in accordance with copyright law implemented in Austria had substantial collateral damage, affecting the reachability for tens of thousands of domains. At the same time, the efficacy of the blocks was limited, as most affected sites were simultaneously reachable via other non-blocked IPv4 addresses or via IPv6. From these observations, we can see that the blocking of specific IP addresses does not fully achieve its goal, while causing substantial collateral damage to uninvolved third parties.

Looking at affected targets—limiting this perspective to entities using domains under the Austrian ccTLD `.at`—we find that several entities with a protected status in a free society were affected. This list includes religious organizations, but also several journalistic offerings. Especially the latter is a serious issue, given the fundamental nature of journalism for a free society. We argue that, given the impact and scale of false positives in this case, possible consequence of allowing entities to (in some cases automatically) request the blocking of specific IP addresses should be carefully considered.

6 CONCLUSION

In this paper we investigated the chain of events around the blocking of Cloudflare IPv4 addresses between the 28^{th} and 29^{th} of August 2022 in Austria. We find that between 5,609 and 63,126 *unique* domains were impacted by the false-positive overblocking, affecting domains of religious entities as well as journalistic offerings. At the same time, the censorship attempt had limited efficacy, as it neither encompassed all service domains of the intended targets, nor involved all IP addresses these sites were operating under. In summary, we find that censorship based on IP addresses in the modern Internet leads to substantial collateral damage of innocent third parties, affecting core values of a free society. As such, it should be carefully considered, whether censorship is a suitable tool in such a free society.

REFERENCES

[1] M. Allman and V. Paxson. 2007. Issues and Etiquette Concerning Use of Shared Measurement Data. In *Proceedings of the 2007 Internet Measurement Conference*. ACM.

[2] Amazon.com, Inc. [n. d.] Alexa Top Sites. Retrieved May 17, 2022 from https://www.alexa.com/.

[3] Anonymous, A. A. Niaki, N. P. Hoang, P. Gill, and A. Houmansadr. 2020. Triplet censors: demystifying great Firewalls DNS censorship behavior. In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI)*.

[4] Anonymous Authors. 2012. The Collateral Damage of Internet Censorship by DNS Injection. *ACM SIGCOMM CCR*, 42, 3.

[5] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. 2005. DNS Security Introduction and Requirements. RFC 4033. IETF, (Mar. 2005). http://tools.ietf.org/rfc/rfc4033.txt.

[6] Argention, M.A. 2022. Twitter Thread on Kiwifarms. (Sept. 5, 2022). Retrieved Oct. 10, 2022 from https://twitter.com/_MAArgentino/status/1566879509453881345.

[7] Austrian Law. 2022. Paragraph 81 Abs. 1a UrhG (Urheberrechtsgesetz, copyright law). (Jan. 28, 2022). https://www.jusline.at/gesetz/urhg/paragraf/81.

[8] K. R. Batch, T. Magi, and M. Luhtala. 2015. Filtering beyond cipa: consequences of and alternatives to overfiltering in schools. *Knowledge Quest*, 44, 1.

[9] K. Bock, P. Bharadwaj, J. Singh, and D. Levin. 2021. Your censor is my censor: weaponizing censorship infrastructure for availability attacks. In *2021 IEEE Security and Privacy Workshops (SPW)*. IEEE.

[10] K. Bock, G. Hughey, X. Qiang, and D. Levin. 2019. Geneva: evolving censorship evasion strategies. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*.

[11] K. Bock, G. Naval, K. Reese, and D. Levin. 2021. Even censors have a backup: examining china's double https censorship middleboxes. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet*.

[12] Y. Breindl and B. Kuellmer. 2013. Internet content regulation in france and germany: regulatory paths, actor constellations, and policies. *Journal of Information Technology & Politics*, 10, 4.

[13] J. Cabal, P. Benáek, L. Kekely, M. Kekely, V. Pu, and J. Koenek. 2018. Configurable fpga packet parser for terabit networks with guaranteed wire-speed throughput. In *Proceedings of the 2018 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*.

[14] A. Chaabane, T. Chen, M. Cunche, E. De Cristofaro, A. Friedman, and M. A. Kaafar. 2014. Censorship in the wild: analyzing internet filtering in syria. In.

[15] D. Cicalese, D. Giordano, A. Finamore, M. Mellia, M. Munafò, D. Rossi, and D. Joumblatt. 2015. A first look at anycast cdn traffic. *arXiv preprint arXiv:1505.00946*.

[16] Cisco Systems. [n. d.] Deep Packet Inspection (vEdge 20 Manual). Retrieved Oct. 10, 2022 from https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge-20-x/policies-book/m-config-deep-packet-inspection.pdf.

[17] Cloudflare. [n. d.] Cloudflare Docs: Time to Live (TTL). Retrieved Oct. 11, 2022 from https://developers.cloudflare.com/dns/manage-dns-records/reference/ttl/.

[18] A. Daffalla, L. Simko, T. Kohno, and A. G. Bardas. 2021. Defensive technology use by political activists during the sudanese revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[19] Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey, J. A. Halderman, and V. Paxson. 2017. The security impact of https interception. In *NDSS*.

[20] D. Eastlake 3rd. 2011. Transport Layer Security (TLS) Extensions: Extension Definitions. RFC 6066. IETF, (Jan. 2011). http://tools.ietf.org/rfc/rfc6066.txt.

[21] Epicenter.Works. 2022. URHEBERRECHTSINDUSTRIE PROVOZIERT SHUTDOWN VON TEILEN DES INTERNETS IN ÖSTERREICH. (Aug. 29, 2022). Retrieved Feb. 27, 2023 from https://epicenter.works/content/urheberrechtsindustrie-provoziert-shutdown-von-teilen-des-internets-in-oesterreich.

[22] Farsight Inc. [n. d.] Farsight - Security Information Exchange (SIE). Retrieved Oct. 11, 2022 from https://www.farsightsecurity.com/solutions/security-information-exchange/.

[23] T. Fiebig and D. Aschenbrenner. 2022. 13 propositions on an internet for a" burning world". In *ACM SIGCOMM 2022 Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet*.

[24] T. Fiebig, K. Borgolte, S. Hao, C. Kruegel, and G. Vigna. 2017. Something from nothing (there): collecting global ipv6 datasets from dns. In *International Conference on Passive and Active Network Measurement*. Springer.

[25] T. Fiebig, S. Gürses, C. H. Gañán, E. Kotkamp, F. Kuipers, M. Lindorfer, M. Prisse, and T. Sari. 2023. Heads in the clouds? measuring universities' migration to public clouds: implications for privacy & academic freedom. *Proceedings on Privacy Enhancing Technologies*, 2023, 2.

[26] P. Foremski, O. Gasser, and G. C. Moura. 2019. Dns observatory: the big picture of the dns. In *Proceedings of the Internet Measurement Conference*.

[27] S. Frolov and E. Wustrow. 2019. The use of tls in censorship circumvention. In *NDSS*.

[28] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger. 2017. Inferring bgp blackholing activity in the internet. In *Proceedings of the 2017 Internet Measurement Conference*.

[29] Google. 2022. Chrome Platform Status: Feature: TLS Encrypted Client Hello (ECH). (Sept. 25, 2022). Retrieved Oct. 16, 2022 from https://chromestatus.com/feature/6196703843581952.

[30] J. L. Hall, M. D. Aaron, A. Andersdotter, B. Jones, N. Feamster, and M. Knodel. 2023. A Survey of Worldwide Censorship Techniques. Internet-Draft draft-irtf-pearg-censorship-09. Work in Progress. Internet Engineering Task Force, (Jan. 2023). 45 pp. https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship/09/.

[31] J. Han, S. Kim, J. Ha, and D. Han. 2017. Sgx-box: enabling visibility on encrypted traffic using a secure middlebox module. In *Proceedings of the First Asia-Pacific Workshop on Networking*.

[32] M. Harrity, K. Bock, F. Sell, and D. Levin. 2022. GET/out: automated discovery of Application-Layer censorship evasion strategies. In *31st USENIX Security Symposium (USENIX Security 22)*.

[33] P. Hoffman and P. McManus. 2018. DNS Queries over HTTPS (DoH). RFC 8484. IETF, (Oct. 2018). http://tools.ietf.org/rfc/rfc8484.txt.

[34] O. Hohlfeld. 2018. Poster: Operating a DNS-based Active Internet Observatory. In *Proc. of the 2018 ACM SIGCOMM Conference (SIGCOMM)*.

[35] R. Houser, S. Hao, Z. Li, D. Liu, C. Cotton, and H. Wang. 2021. A comprehensive measurement-based investigation of dns hijacking. In *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*. IEEE.

[36] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman. 2016. Specification for DNS over Transport Layer Security (TLS). RFC 7858. IETF, (May 2016). http://tools.ietf.org/rfc/rfc7858.txt.

[37] C. Huitema, S. Dickinson, and A. Mankin. 2022. DNS over Dedicated QUIC Connections. RFC 9250. IETF, (May 2022). http://tools.ietf.org/rfc/rfc9250.txt.

[38] ICANN. [n. d.] ICANN TLD Statistics. Retrieved Oct. 11, 2022 from https://magnitude.research.icann.org/.

[39] K. Jacobs. 2021. Encrypted Client Hello: the future of ESNI in Firefox. (Jan. 7, 2021). Retrieved Oct. 16, 2022 from https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/.

[40] C. Jarvis. 2020. *Crypto Wars: The Fight for Privacy in the Digital Age: a Political History of Digital Encryption*. CRC Press.

[41] L. Jin, S. Hao, H. Wang, and C. Cotton. 2021. Understanding the impact of encrypted dns on internet censorship. In *Proceedings of the Web Conference 2021*.

[42] S. C. Jones, J. A. Thom, S. Davoren, and L. Barrie. 2014. Internet filters and entry pages do not protect children from online alcohol marketing. *Journal of public health policy*, 35.

[43] Juniper. 2018. DPI Script Service Overview (Service Management on SRC-Managed Routers). (Sept. 20, 2018). Retrieved Oct. 10, 2022 from https://www.juniper.net/documentation/en_US/src4.13/topics/concept/sae-devices-dpi-script-service-overview.html.

[44] E. Kenneally and D. Dittrich. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. *Available at SSRN 2445102*.

[45] Laura Wood. 2022. Global Deep Packet Inspection (DPI) Market Report 2022: Market to Reach $13.1 Billion by 2026 - DPI Deployments Soar Amid Growing Emphasis on Network Security. (Jan. 28, 2022). Retrieved Oct. 10, 2022 from https://www.globenewswire.com/en/news-release/2022/01/28/2374926/28124/en/Global-Deep-Packet-Inspection-DPI-Market-Report-2022-Market-to-Reach-13-1-Billion-by-2026-DPI-Deployments-Soar-Amid-Growing-Emphasis-on-Network-Security.html.

[46] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, and W. Joosen. 2019. Tranco: a research-oriented top sites ranking hardened against manipulation. In *Network and Distributed Systems Security (NDSS) Symposium 2019*.

[47] H. Li, J. Zhang, and R. Sarathy. 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48, 4.

[48] B. Liu, C. Lu, Z. Li, Y. Liu, H.-X. Duan, S. Hao, and Z. Zhang. 2018. A reexamination of internationalized domain names: the good, the bad and the ugly. In *DSN*.

[49] LIWEST. 2022. Netzsperren LIWEST. (Aug. 28, 2022). Retrieved Oct. 10, 2022 from http://web.archive.org/web/20220828220559/http://netzsperre.liwest.at/.

[50] F. Madenga. 2021. From transparency to opacity: storytelling in zimbabwe under state surveillance and the internet shutdown. *Information, Communication & Society*, 24, 3.

[51] A. McDonald, M. Bernhard, L. Valenta, B. VanderSloot, W. Scott, N. Sullivan, J. A. Halderman, and R. Ensafi. 2018. 403 Forbidden: a global view of CDN geoblocking. In *Proceedings of the Internet Measurement Conference 2018*.

[52] T. J. McIntyre. 2010. Blocking child pornography on the internet: european union developments. *International Review of Law, Computers & Technology*, 24, 3.

[53] Mozilla Foundation. [n. d.] Public Suffix List. Retrieved Oct. 11, 2022 from https://publicsuffix.org/.

[54] C. Patton. 2020. Good-bye ESNI, hello ECH! (Dec. 8, 2020). Retrieved Oct. 16, 2022 from https://blog.cloudflare.com/encrypted-client-hello/.

[55] V. Paxson. 1999. Bro: a system for detecting network intruders in real-time. *Computer networks*, 31, 23-24.

[56] J. Poort, J. Leenheer, J. van der Ham, and C. Dumitru. 2014. Baywatch: two approaches to measure the effects of blocking access to the pirate bay. *Telecommunications Policy*, 38, 4.

[57] J. Quintais. 2020. The new copyright in the digital single market directive: a critical look. *European Intellectual Property Review*.

[58] R. Radu and M. Hausding. 2020. Consolidation in the dns resolver market–how much, how fast, how dangerous? *Journal of Cyber Policy*, 5, 1.

[59] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood. 2022. Draft RFC: TLS Encrypted Client Hello. (Oct. 3, 2022). Retrieved Oct. 16, 2022 from https://datatracker.ietf.org/doc/draft-ietf-tls-esni/.

[60] P. Richter, O. Gasser, and A. Berger. 2022. Illuminating large-scale ipv6 scanning in the internet. In *Proceedings of the Internet Measurement Conference*.

[61] RIPE Atlas. 2022. Ripe atlas measurement 44194385. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194385/.

[62] RIPE Atlas. 2022. Ripe atlas measurement 44194663. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194663/.

[63] RIPE Atlas. 2022. Ripe atlas measurement 44194664. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194664/.

[64] RIPE Atlas. 2022. Ripe atlas measurement 44194665. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194665/.

[65] RIPE Atlas. 2022. Ripe atlas measurement 44194666. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194666/.

[66] RIPE Atlas. 2022. Ripe atlas measurement 44194667. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194667/.

[67] RIPE Atlas. 2022. Ripe atlas measurement 44194668. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194668/.

[68] RIPE Atlas. 2022. Ripe atlas measurement 44194669. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194669/.

[69] RIPE Atlas. 2022. Ripe atlas measurement 44194670. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194670/.

[70] RIPE Atlas. 2022. Ripe atlas measurement 44194671. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194671/.

[71] RIPE Atlas. 2022. Ripe atlas measurement 44194672. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194672/.

[72] RIPE Atlas. 2022. Ripe atlas measurement 44194673. (Aug. 29, 2022). Retrieved Sept. 24, 2022 from https://atlas.ripe.net/measurements/44194673/.

[73] RIPE NCC. 2022. RIPE NCC Response to Request from Ukrainian Government. (Mar. 10, 2022). Retrieved Oct. 10, 2022 from https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government.

[74] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy. 2015. Blindbox: deep packet inspection over encrypted traffic. In *Proceedings of the 2015 ACM conference on special interest group on data communication*.

[75] S. Singanamalla, S. Chunhapanya, M. Vavrua, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. Wood. 2020. Oblivious dns over https (odoh): a practical privacy enhancement to dns. *arXiv preprint arXiv:2011.10121*.

[76] A. Starzak and M. Fayed. 2022. The unintended consequences of blocking IP addresses. (Dec. 16, 2022). Retrieved Feb. 2, 2023 from https://blog.cloudflare.com/consequences-of-ip-blocking/.

[77] F. Streibelt, J. Böttger, N. Chatzis, G. Smaragdakis, and A. Feldmann. 2013. Exploring edns-client-subnet adopters in your free time. In *Proceedings of the 2013 conference on Internet measurement conference*.

[78] R. Sundara Raman, P. Shenoy, K. Kohls, and R. Ensafi. 2020. Censored planet: an internet-wide, longitudinal censorship observatory. In *proceedings of the 2020 ACM SIGSAC conference on computer and communications security*.

[79] M. C. Tschantz, S. Afroz, V. Paxson, et al. 2016. Sok: towards grounding censorship circumvention in empiricism. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[80] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid. 2018. Data exfiltration: a review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, 101.

[81] O. van der Toorn, R. van Rijswijk-Deij, T. Fiebig, M. Lindorfer, and A. Sperotto. 2020. TXTing 101: Finding Security Issues in the Long Tail of DNS TXT Records. In *Proceedings of the International Workshop on Traffic Measurements for Cybersecurity (WTMC)*.

[82] B. VanderSloot, A. McDonald, W. Scott, J. A. Halderman, and R. Ensafi. 2018. Quack: scalable remote measurement of application-layer censorship. In *27th USENIX Security Symposium (USENIX Security 18)*.

[83] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras. 2016. A high-performance, scalable infrastructure for large-scale active dns measurements. *IEEE Journal on Selected Areas in Communications*, 34, 6.

[84] Various Authors. 2022. HackerNews Thread on Austrian Internet Blocking. (Aug. 28, 2022). Retrieved Oct. 10, 2022 from https://news.ycombinator.com/item?id=32630757.

[85] Various Authors. 2022. Multistakeholder Imposition of Internet Sanctions. (Mar. 10, 2022). Retrieved May 12, 2022 from https://www.pch.net/resources/Papers/Multistakeholder-Imposition-of-Internet-Sanctions.pdf.

[86] D. Wang and G. Mark. 2015. Internet censorship in china: examining user awareness and attitudes. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 22, 6.

[87] Z. Wang, Y. Cao, Z. Qian, C. Song, and S. V. Krishnamurthy. 2017. Your state is not mine: a closer look at evading stateful internet censorship. In *Proceedings of the 2017 Internet Measurement Conference*.