Resolving the future: The DNS Layer and the Power to Navigate the Internet

DIGITAL MEDUSA

DIIF

DIGITAL MEDUSA

DIGITAL
/NFRASTRUCTURE
/NSIGHTS
FUND

Digital Medusa – March 2025

Author: Farzaneh Badiei
Data Engineer: Sebastian Castro

Acknowledgment:
This report was made possible by the contributions of Digital Medusa collaborators, especially Angie Orejuela. We would also like to thank the stakeholders who shared their insights and participated in interviews. Special thanks go to Digital Infrastructure Insights Funds for supporting this project.

Summary

This research explores the alleged shift towards the consolidation of DNS services into a handful of large providers. The research aims to understand the extent of this consolidation, its potential implications, and the factors driving this trend.

Interviews with DNS stakeholders were conducted with representatives from various organizations involved in the DNS, including Internet Corporation for Assigned Names and Numbers, Public Interest Registry, Internet Society, Quad9, EasyDNS, and others, to gather insights on the current state of DNS and potential areas for improvement.

The qualitative part of the research focuses on interview responses and desk research. The quantitative part focuses on monitoring the trend of adoption of public DNS resolvers by Internet Service Providers.

Regulatory landscape: DNS resolver operators face complex regulatory challenges due to varying laws and regulations globally. Privacy, blocking and filtering requirements, and compliance with extraterritorial laws pose significant hurdles, particularly for non-profit operators. We decided to provide a DNS resolver blocking tracker for the community to use.

Open-source adoption: Interviewees generally expressed no concerns about using open-source software for DNS resolvers. However, challenges related to scalability and finding suitable open-source solutions for large-scale operations were noted.

DNS resolver blocking: The research highlights instances of DNS resolver blocking by governments worldwide, often for censorship or content control purposes. DNS resolver blocking can be one of the drivers of consolidation.

Data analysis: Analysis of APNIC DNS resolver data revealed a global decline in the use of public DNS resolvers by ISPs and network operators. However, regional variations and correlations with Internet freedom and political events were observed. It seems that in Central Asia and Western Africa, where Internet freedom was lower, the usage of public DNS resolvers was higher.

Our research might contribute to the diversification of our data sources when researching DNS in general. Sebastian Castro, from .IE., conducted the majority of the data analysis, while Farzaneh Badiei, from Digital

Medusa, undertook the interviews and policy analysis. We are very grateful for Angie Orejuela's research assistance.

Introduction

The Internet and especially its infrastructure is at an important juncture: its critical and core elements are provided by large and well established tech companies. Monitoring the dominance of these platforms in providing the critical infrastructure of the Internet is important . While centralization and consolidation of services might not be detrimental in all cases, it might be preventable and so avoiding centralization might be better for the health of the Internet. This is why we decided to focus this research on one of the most important components of Internet infrastructure: Domain Name System Resolvers.

The Domain Name System (DNS) is a critical component of the Internet, responsible for translating human-readable domain names into machine-readable IP addresses. Traditionally, DNS resolution was a decentralized process handled by numerous independent resolvers. However, in recent years, there has been some evidence that there might be a shift towards the consolidation of DNS services into a handful of large providers, a phenomenon known as "Big DNS."

One reason for such consolidation could be that the Internet Service Providers and Network Operators refer their customers to these public resolvers. Radu et al argue that Internet Service Providers (ISPs) use public resolvers such as Cloudflare and GoogleDNS because it can be less costly. Among Internet experts, the dominant argument is also that ISPs consistently use public DNS resolvers instead of providing their own and this contributes to the consolidation of the DNS resolver market. (See for example this APNIC blog in 2019.) There might be other reasons that contribute to the centralization and consolidation process, which in this research we will explore.

Through this study we want to have a good understanding of theextent to which consolidation is happening, where it is happening, whether it is bad for the Internet and how we can monitor it, slow it down and return it to being decentralized, if desirable. To achieve these goals, we address several questions:

1) Is there a trend in ISPs and network operators using public resolvers globally?

2) What is the pattern of adoption of public DNS resolvers around the world?
3) Is there a dominant DNS resolver in the market?
4) Why do we have only a handful of trusted and popular DNS resolvers?

The research aims to understand the trend of adoption of DNS resolvers and the factors driving this trend and explores its implications for Internet users, businesses, and policymakers.

What are DNS resolvers and why are they important?

Everyday when we connect to the Internet we connect to a DNS resolver. This part of Internet infrastructure is of utmost importance in daily connectivity to the Internet services we want to access. DNS resolvers are a part of the DNS servers which include recursive DNS resolvers, authoritative servers, root nameservers and Top Level Domain name servers. (Cloudflare, What are the different types of DNS server?) DNS recursive resolvers are the intermediaries that receive the user's query and (to put it in a colloquial way) run with it to find the IP address and connect the user to the service through the user's "stub resolver." The DNS recursive resolvers are critical to our access as they are the intermediary we rely on to fetch the IP address and respond to our query and subsequently enable us access to the online service and platforms. If our DNS resolvers do not work or do not work reliably, we might not be able to access web services or other online services. An example of this can be found in a news piece by Western Africa Telecom. Despite the fact that the telecom operator had all the infrastructure in place and provided Caching and other solutions, due to the sub-optimal DNS resolvers, the Caching still did not enhance the customers' experience as their queries were resolved through public resolvers that had high latency. (CacheBox and DNSBox enhance experience in Liberia.) Poorly configured DNS resolvers are one of the major reasons for sub-optimal connectivity and access to web services. (See CAIDA study.)

"Public resolvers" are resolvers that answer queries from outside the resolver's own network (in contrast to the resolvers offered by ISPs, which are normally restricted just to the ISP's own customers). Since at least 2009, various corporations have provided public resolvers to people who wanted an alternative to the resolvers provided by their ISP. Sometimes (especially among the technical community) the terms "open resolvers" and "public resolvers" are used interchangeably.

What do we mean by consolidation, centralization and concentration?

A cursory review of the field that works on issues such as consolidation and centralization reveals that these terms are used interchangeably. (See Internet Society's report.) In this report we also use the terms consolidation and centralization. However, there are subtle differences between centralization and consolidation. Concentration reflects the extent to which market power and control are concentrated in a few entities, often as a result of consolidation. Consolidation refers to the trend of services and infrastructure on the Internet becoming concentrated in the hands of a few large providers. Centralization is the outcome of consolidation of services. In essence, consolidation is the trend or process of moving toward a more concentrated market, while centralization is the resulting state of affairs where fewer entities control critical resources and service. Some research suggests that concentration of services is happening more visibly at the DNS layer which goes against its decentralized nature. (Internet Society Report.)

Research Process, Methodology

Our research process involves a mixed method approach of qualitative and quantitative analysis as well as extensive desk research. We conducted in-depth interviews with representatives from a diverse range of organizations in the DNS ecosystem located in various parts of the world.

The Qualitative Analysis

The qualitative analysis included desk research and interviews. To establish the incentives and deterrents of adopting third party public DNS resolvers and open source DNS resolvers, we used the Transaction Costs Economics theory (by Williamson) and used the past academic and industry literature about the adoption of public DNS resolvers. We also conducted interviews to contextualize and corroborate some of the studies.

Organizations Interviewed

In identifying the organizations to interview, we looked at civil society organizations that worked on Internet infrastructure (such as the Internet Society) and Internet Service Providers and DNS resolver operators. We interviewed sixteen representatives from the following organizations:

Name	Website	Type	Region
Quad9	https://www.quad9.net	DNS Provider	Global
CIRA	https://www.cira.ca	Internet Registry/DNS Provider	Canada
Public Interest Registry (PIR)	https://www.pir.org	Non-Profit Organization	Global
Internet Society (ISOC)	https://www.Internetsociety.org	Non-Profit Organization	Global
EasyDNS	https://www.easydns.com	Privately-Owned DNS Provider	Canada
OpenDNS	https://www.opendns.com	Privately-Owned DNS Provider	USA
Comcast	https://www.comcast.com	Telecommunications Company	USA
Whalebone	https://www.whalebone.io	Privately-Owned DNS Provider	Czech Republic
PowerDNS	https://www.powerdns.com	Privately-Owned DNS Software Provider	Netherlands
DNS4ALL	https://dns4all.eu/	Non-Profit Organization	Experimental/Global
Internet Corporation for Assigned Names and Numbers (ICANN)	https://www.icann.org	Non-Profit Organization	Global
Bangladesh Internet Service Provider	BDCOM https://www.bdcom.com/	Internet Service Provider	Bangladesh
Liquid	https://www.liquid.tech	Internet Service Provider	Africa
Vercara	https://www.vercara.com	DNS Provider	Global
Digital Economy Advisors	www.digitaleconomy.ke	Consultancy	Africa
Thomas Rickert	Rickert Law	Legal services for Internet infrastructure	Europe
Karsolink, 2S Computers Srl		Internet Service Provider	Europe

Interview Process

Each interview was conducted online, in person or via email and lasted approximately 30 to 90 minutes. Interviews were semi-structured, allowing us to explore specific topics of interest while also giving interviewees the opportunity to share their thoughts and insights.

The composition of interviewees

During this research we interviewed stakeholders from DNS resolver providers, and nonprofit organizations that work on Internet infrastructure. Our aim was to understand the incentives and deterrents of these organizations when it comes to providing DNS resolver services or to understand their perspective on the adoption of public resolvers or providing their own DNS resolvers. We also focused on what factors usually influence their decision to adopt open source software.

Overview of the Regulatory Landscape

We addressed the regulatory landscape that applied to DNS resolvers through a qualitative method of interviewing several DNS resolvers and ISPs and also undertaking extensive desk research.

The regulatory environment governing DNS resolvers is complex and shaped by two primary factors: nation-states' desires to censor and block content, and the imperative to maintain DNS security and privacy.

These factors often interact in conflicting ways. For example, a government's desire to block gambling or politically sensitive content or apply its local laws may prioritize censorship over privacy, security, resiliency and connectivity, leading to broad DNS-level blocking that impacts user trust and security. Conversely, efforts to enhance DNS security through privacy-respecting technologies, like DNS-over-HTTPS (DoH), can undermine state-level censorship by enabling users to bypass filters, creating tension between regulatory goals (assertion of digital sovereignty) and technical capabilities.

Governments, both democratic and authoritarian, have increasingly leveraged DNS blocking and filtering to enforce national laws, such as blocking gambling websites or politically sensitive content. For instance, in Greece, DNS filtering was employed to block unlicensed gambling websites under national policies, as documented by Ververis in a 2015 study. Similarly, as Singh, Grover and Bansal in a 2020 study explain, countries like India have implemented DNS-level blocking to restrict access to platforms hosting politically sensitive material, illustrating how such measures are applied across varying contexts. Internet censorship at the DNS level has become a prominent tool for implementing such measures because it is relatively cost-effective, easy to implement, and allows governments to enforce content restrictions without directly interfering with user devices or applications.

Mandated local DNS resolvers: One of the research questions that we asked and focused on was whether the ISPs have a mandate to provide their own DNS resolver. Except for one network operator in Italy, almost all of our interviewees mentioned that they were not mandated to do so. However, some mentioned that governments' regulatory blocking and filtering might oblige them to move to a government mandated DNS resolver like DNS4EU to be able to comply with the increasing blocking orders. DNS4EU was formed after the The European Union issued a tender for the candidates to apply to provide a DNS recursive resolver, under the Digital strand of the Connecting Europe Facility (CEF). This kind of initiative is also a continuation of Europe's desire to assert "digital sovereignty" as Radu explains in her study in about DNS4EU (Radu 2023).

Blocking and filtering: Laws and regulations that relate to blocking at the DNS level differ based on the actors (whether they are DNS resolver providers, or ISPs or just the software provider). When we interviewed Telecommunications companies, for example, they mentioned that if they provide blocking web services directly for residential consumers, they might face Net Neutrality related challenges. Net Neutrality policies in the US are "a national standard by which we ensure that broadband Internet service is treated as an essential service. It prohibits Internet service providers from blocking, throttling, or engaging in paid prioritization of lawful content." Nevertheless, if there is a court order that asks the ISPs to block certain websites, they need to oblige. We have not come across a hard coded law that obliges "DNS resolvers" specifically to get engaged with blocking. However, as we mention in the next section, there are court orders against DNS resolvers to block access and Italy Piracy Shield.

Some other network operators might be obliged by the law to block online services. For example, in the UK, according to the Digital Economy Act 2017, ISPs are required to filter domain names and block access to pornographic websites and have appropriate age verification in place.

Legal Cases and Precedents

Laws and court orders might directly apply to DNS resolvers. In April 2022, U.S. District Judge Katherine Polk Failla of the Southern District of New York issued a significant ruling targeting online piracy. The court in the US ruled that all the ISPs should block access to three domain names that hosted infringing materials. The ruling was perceived as the broadest injunction on Internet issues ever seen in US history, as the judges are usually much more careful in the US due to first amendment considerations. The injunction included blocking at the DNS server and DNS resolver level as well as orders of domain name takedown to domain name registries and registrars. The ruling was so broad that the Electronic Frontier Foundation, Computer Communications Industry Association (CCIA) and Cloudflare filed an Amicus Brief.

While it seems like the injunction (as a result of the Amicus Brief) became more precise, it is still in place and it is not clear whether and how Cloudflare or other public resolvers are following the injunction. When visiting Israel.tv with multiple DNS resolvers we see: "On 26 April 2022 the Honorable District Court Judge Failla has issued a judgment that includes an order to block all access to this website / service due to copyright infringement".

This case is highly important in the DNS resolver blocking debate as the Judge did not only oblige the telecom operators to block the domain names, but the DNS resolvers specifically have to comply with the blocking order.

DNS resolvers' reactions to lawsuits (which are usually brought by copyright holders) have been different. In some cases, DNS resolvers have stopped serving the jurisdiction that demands blocking domain names due to copyright infringement. OpenDNS stopped serving France after the court ruled in favor of Canal+ to block domain names. Google, on the other hand, followed the ruling and reports that it does undertake blocking in France. (Google Blocking Policy)

Google announced: "Copyright laws in some jurisdictions allow rights holders to seek judicial injunctions against DNS intermediaries that require those intermediaries to block specified copyright infringing domains in those jurisdictions. For these jurisdictions, Google Public DNS will comply with court orders to block DNS resolution of all names under specified domains. In the event of a block, we will communicate this explicitly in the query response. The response returned will have DNS RCODE REFUSED, optionally with an extended DNS error 16 (Censored)."

Quad9, on the other hand, contests these rulings and, as reported in Torrent Freak (2024), explains that "Quad9 system is designed to treat every user in every country the same way. For privacy reasons, Quad9 also has no precise information about the location of its users. Therefore, to remain in compliance, we have to block these sites for all users, in all areas. This amounts to French law being applied globally. When we interviewed software providers for DNS resolvers, they mentioned that because they do not deal with the data themselves and do not resolve the queries directly they are not obligated to follow a specific regulation or a law; but because their customers might have to, they provide certain services that enable their customers to undertake blocking and filtering or install parental control. (Interview with PowerDNS.) A DNS resolver operator based in Europe mentioned that they have to provide blocking for unlicensed gambling websites in the Czech Republic and follow General Data Protection Regulation. It seems that the Czech Republic Gambling Act extends to Internet Service Providers (Whalebone). The Gambling Act went into effect in 2017 and blocking the domain was challenged in the Czech Republic constitutional court, but it was ruled that domain name blocking is not unconstitutional and ISPs should be a part of the process and block the domain name of unauthorized services. (Czech Republic Constitutional Court Judgement, Pl. US 28/16, 14 February 2017.)

Privacy: Most of the interviewees that operate DNS resolvers mentioned that they have to follow data protection laws and regulation (in different regions, as well as the US, the EU, Australia and Canada) but they also mentioned that they follow the IETF privacy and security standards for running DNS resolvers, RFC8932.

Exemptions: It is possible that some jurisdictions consider an exemption for DNS resolver providers and not consider them asTelecommunications Service Providers. Switzerland, for example, has issued a specific statement for Quad9 (a DNS resolver provider) announcing that "In conclusion, we confirm that Quad9 is not subject to the SPTA in providing its DNS resolver service and therefore is not required to fulfill any obligations under the SPTA and its implementing ordinances." (Quad9 Transparency Report.) As explained later in this report, exemptions might not have extraterritorial effects.

Compliance with extraterritorial laws: DNS resolver operators have been increasingly dealing with complex regulatory issues since they operate globally. The complexity stems from the fact that not only DNS resolver providers have to comply with their local laws and regulations, other regulatory frameworks and laws in other jurisdictions but also they are applicable to the resolvers. This can result in DNS resolvers being sued, for example, due to the copyright infringement that their customers carry out. As mentioned, some recent cases concern Quad9, OpenDNS and Cloudflare lawsuits in France, Portugal and Italy.

The increasing legal pressure especially creates hurdles for nonprofit DNS resolver operators such as Quad9. Noncommercial operators do not have access to resources to fight these battles internationally in court. The regulatory pressure on DNS resolvers can be divided into the following:

> Telecommunications, Cybersecurity, Gambling and Online Safety laws that a country applies to the DNS resolvers and does not exempt the resolvers specifically from those laws

Governments and other entities orders and actions that could affect DNS resolvers operations such as Blocking orders and redirect of DNS queries through ISPs

The Battle of Quad9

The Quad9 case stands as a prime illustration of the legal and operational hurdles encountered by DNS resolver operators, particularly those that emphasize privacy and security without resorting to content censorship. This expanded analysis focuses on the intricacies of the Quad9 case, drawing upon the provided sources.

The Initial Legal Challenge:

Sony's Demand and the Preliminary Injunction: The legal battle commenced when Sony Music Entertainment Germany demanded that Quad9 cease resolving two domain names allegedly hosting copyrighted material. This demand led to a Hamburg, Germany court issuing a preliminary injunction against Quad9, mandating the blocking of the specified domain names (Quad9 report).

Extraterritoriality, Jurisdictional Considerations and Quad9's Objection: The court's jurisdiction extended to Switzerland, Quad9's registered office, through the Lugano Treaty. Quad9 contested the injunction, asserting that as a telemedia service provider, they were exempt from such blocking requests under the German Telemedia Services Act (TMSA), the precursor to the Digital Services Act (DSA). The TMSA provides certain legal protections and exemptions for telemedia service providers (Quad 9 report).

Court's Decision and Rationale:

Rejection of Telemedia Service Status and Upholding of the Injunction: The Hamburg court ruled against Quad9, determining that they did not qualify as a telemedia service provider and thus were not entitled to the legal privileges under the TMSA. Consequently, the court upheld the preliminary injunction, compelling Quad9 to block the domain names. This decision hinged on the court's interpretation of the TMSA and its applicability to DNS resolver services.

The Second Court Case and its Repercussions:

Leipzig ruling: When escalated to Leipzig court, the court decreed that

Quad9 must cease resolving the domain names, classifying them as a "disturber" under German law—a legal construct for those involved in another party's infringement. The court determined that Quad9's blocking efforts were insufficient and imposed a financial penalty for non-compliance.

Circumvention and Geographic Blocking Challenges: The court's decision encountered complications due to German mobile network operators routing specific requests to data centers in neighboring countries where the blocking measures were not enforced. This highlighted the challenges of implementing geographic blocking and the potential for circumvention.

Dresden Victory

Quad9 appealed the decision in Leipzig, and the higher regional court in Dresden overturned the lower court's decision, meaning Quad9 ultimately won the case.

Key Issues and Concerns:

- **Disproportionate Burden on DNS Resolvers and Impact on Free Speech:** The case underscored how copyrights holders could inundate numerous independent DNS resolver operators with blocking requests, imposing a substantial burden on them. This could compel resolver operators to choose between costly legal battles or implementing blocks, potentially stifling undesired speech without legal recourse to verify the block's legitimacy or proportionality.
- **Proportionality and Geographic Blocking Concerns:** The practice of blocking entire domains raises proportionality concerns, as it cuts off access to all services under that domain. Furthermore, the case illustrated how a court in one jurisdiction could impose a blocking order affecting users in other jurisdictions, raising questions about the territorial scope of such orders.

How can DNS resolvers fight with DNS blocking court orders?

In its fight with unfair and disproportional court orders that can affect the integrity of the web and the Internet, Quad9 has been exemplary. It has maintained transparency regarding the blocking orders they receive:

- **Transparency, Privacy, and No Content Censorship:** Quad9 has maintained transparency regarding the requests they receive, operating under stringent Swiss privacy guidelines that prohibit storing user IP addresses or associating them with queries. They uphold a no-content-censorship policy, viewing attempts to regulate content access as a threat.

- **Global Operations and Non-Profit Status:** With operations in over 230 locations globally, Quad9 prioritizes deploying servers close to the network edge. Their non-profit status facilitates partnerships with multiple threat intelligence providers, bolstering their security capabilities and globally providing their services.
- **Advocacy and Legal Challenges:** Quad9 advocates for a structured blocking implementation approach to aid courts in determining appropriate requests. They are prepared to legally challenge blocking orders and have successfully appealed certain decisions.

6. Overarching Concerns and Global Trends:

- **Legal Pressure, Regulatory Complexity, and Jurisdictional Issues:** The case exemplifies the mounting legal pressure on DNS resolvers, especially non-profit entities. DNS resolvers grapple with intricate regulatory landscapes due to diverse global laws and jurisdictional challenges concerning courts' authority over resolvers operating across borders.
- **Extraterritoriality and the Global Trend Towards DNS-Level Blocking:** Exemptions within one country might not have extraterritorial effects. The case highlights a global trend towards content takedowns or blocking at the DNS resolver level, raising concerns about centralized control and potential censorship.

7. The Importance and Implications of the Case:

- **Precedent, Transparency, and the Need for International Cooperation:** The Quad9 case sets a precedent for potential future targeting of DNS resolvers by courts and rights holders. Quad9's transparency and willingness to fight the case serve as a positive model for other resolvers (see their full report here). The case underscores the necessity for international collaboration to address these challenges and safeguard users' access to content while respecting their human rights.

In essence, the Quad9 case encapsulates the tensions between copyright enforcement, Internet freedom, and the role of DNS resolvers. This case carries significant ramifications for the future of DNS and the Internet as a whole, prompting crucial questions about content regulation, jurisdiction, and user rights. It emphasizes the need to strike a balance between protecting intellectual property and upholding Internet freedom, ensuring that DNS resolvers can operate in a manner that respects both principles.

Italy's Piracy Shield

One of the most controversial laws that directly affects blocking and filtering at the DNS resolver level is the Italian Piracy Shield. According to this law, ISPs and DNS resolvers are required to block copyright infringing domain names and IP addresses associated with illegal streaming within 30 minutes of receiving a notification from authorities. The authority that is responsible for filing the complaint is Autorità per le Garanzie nelle Comunicazioni (AGCOM). In December 2024, the Italian court ruled (for a summary refer to Previti) that Cloudflare and other providers were obliged to block pirated domains. Recently (in March 2025) since Google did not respond to the AGCOM complaint about a copyright infringing livestreaming domain name, AGCOM took Google to court in Milan which was ordered in favor of AGCOM and the court in this case also said that the Piracy Shield law applies to various services including DNS services.

In early January 2025, CCIA- Europe issued a statement that expressed concerns about this law to the EU. In the statement it recounted that as a result of this disproportionate and sweeping law, in October access to some of the services that were not committing piracy such as YouTube and Google Drive for some users in Italy was blocked. They also criticize the law's lack of transparency.

DNS Resolver Blocking Global Tracker

Region	Country	Incident Description	DNS Resolvers Involved	Type	Year	Relevant Links	Outcome
Asia	Turkey	Government censorship leading to blocking of Google DNS and OpenDNS and hijacking their traffic	Google DNS, OpenDNS	Government action	2014	https://www.Internetsociety.org/blog/2014/04/turkish-hijacking-of-dns-providers-shows-clear-need-for-deploying-bgp-and-dns-security; https://www.bortzmeyer.org/dns-routing-hijack-turkey.html#:~:text=A%20new%20step%20in%20the,resolvers%2C%20like%20Google%20Public%20DNS.	Temporary censorship
Asia	Russia	Government censorship leading to DNS resolver blocking	Local ISPs, Yandex DNS	Government action	2017	Reported by Mikhail Klimarev https://t.me/zatelecom/18853 (The partial blocking of Google and Cloudflare DNS services was also reported on a Telegram channel run by Mikhail Klimarev, an expert of the Internet Defense Society He noted that the WireGuard VPN protocol was also completely blocked.) https://github.com/net4people/bbs/issues/81?	Temporary censorship
Europe	Austria	Court-ordered ISPs to block infringing copyright materials	Cloudflare IP addresses	Government (Court)	2022	https://blog.cloudflare.com/consequences-of-ip-blocking	Temporary service disruption to thousands of websites
Europe	Italy	Cloudflare ordered to block websites	Cloudflare	Government (Court)	2022	https://www.ilsole24ore.com/art/lotta-pirateria-musicale-le-major-vittoria-italia-contro-cloudflare-AEaYDFnB?refresh_ce=1; https://torrentfreak.com/court-orders-cloudflares-dns-resolver-1-1-1-1-to-block-pirate-sites-in-italy-220719/	Cloudflare's appeal against DNS-blocking injunction rejected
Europe	Germany	Cloudflare and CDN were ordered to block infringing websites	Cloudflare	Government (Court)	2023	Cloudflare liable for copyright infringement by providing CDN services but not for DNS resolver services - The IPKat. https://blog.cloudflare.com/latest-copyright-decision-in-germany-rejects-blocking-through-global-dns-resolvers/ The Higher Regional Court of Cologne partially upheld the appeal (case 6 U 149/22). It	Cloudflare's appeal was accepted for DNS resolver services

						found that Cloudflare was liable for copyright infringement due to providing the CDN services but not for the DNS resolver services.	
Latin America	Brazil	ISPs blocked access to WhatsApp via DNS manipulation	Local ISPs	Government action	2015	https://ooni.org/post/whatsapp-blocked-in-brazil/	Block was lifted
Asia	Jordan	Government censorship blocking Clubhouse	Local ISPs	Government	2021	https://josa.ngo/blog/78	Block was lifted
Asia	Malaysia	DNS hijacking redirected traffic to local ISPs	GoogleDNS, Cloudflare	Government	2024	https://imap.sinarproject.org/reports/2024/transparent-dns-proxy-implemented-in-malaysia/	Ongoing
Asia	Malaysia	Government requested ISPs to block three domain names	Local ISP DNS resolvers	Government	2018	https://www.malaymail.com/news/malaysia/2018/05/09/mcmc-says-censored-sites-providing-ge14-live-results-to-preserve-public-order/1635402	Domain names remain blocked
Europe	France	Court order for DNS poisoning to block piracy circumvention	Google, Cloudflare, Cisco	Government (Court)	2024	https://torrentfreak.com/google-cloudflare-cisco-will-poison-dns-to-stop-piracy-block-circumvention-240624/	Google complied with the blocking order
Europe	Germany	Sony sued Quad9; court ruled in favor of Sony but Quad9 appealed	Quad9	Government (Court)	2023	https://www.techdirt.com/2023/05/12/good-and-bad-news-on-attempts-to-implicate-dns-services-for-copyright-infringement-at-the-domains-they-resolve/; https://www.quad9.net/uploads/URT_05_12_2023_en_Korr_MH_en2_2e629b1f7b.pdf	Quad9 won the appeal
Europe	Italy	Italian authority AGCOM and the authority have filed a lawsuit against Google, invoking the Piracy Shield	Cloudflare, Google	Court	2025	https://arstechnica.com/gadgets/2025/03/italian-court-orders-google-to-block-iptv-pirate-sites-at-dns-level/	The court in Milan ruled that Google should start blocking domain names that carry pirated materials. Google can appeal this ruling
Americas	USA	Injunction held against DNS resolvers to block certain websites	Cloudflare	Court	2022	https://casetext.com/case/united-king-film-distribution-ltd-v-does-1?__cf_chl_tk=QvRyvY8AdzrCuYaZpDk_3.SEwEnk16ODflcjmh0Q4M4-1740202384-1.0.1.1-Uu4lpT4lWGK7MblovFcFDLTLi6.0rrqZQ70hSWqt5MI	Injunction refined following amicus briefs

- The negative effects of blocking domain names and DNS resolvers

The Internet Engineering Task Force (IETF) is responsible for standardizing the technical operations of the Internet through various standards. In 2016, the Internet Architecture Board (IAB) published RFC 7754, titled "Technical Considerations for Internet Service Blocking and Filtering," which examines the increasing emphasis on blocking and filtering mechanisms designed to restrict access to abusive or objectionable content.

The authors of RFC 7754 suggest that, when feasible, the approach most consistent with Internet architecture is to inform endpoints about potentially undesirable services, enabling users to avoid engaging in such communications. They note that blocking can target specific content, services, endpoints, or combinations thereof, and that blocking systems vary in design, operating at either the Internet Protocol (IP) level or the Domain Name System (DNS) level.

When blocking occurs at the DNS level by restricting the use of certain domain names, all services provided by the hosts associated with those names—including email and web services—are affected. The authors point out that this form of blocking can have unintended consequences on other communication services, rendering it disproportionate and imprecise.

Many technical experts warn against filtering and blocking at the DNS level. One of their arguments against filtering and blocking domain names is that it is ineffective: Read this interesting piece by Bortzmeyer, one of the most prominent DNS experts. To circumvent filtering and blocking tools that are usually used among communities with oppressive regimes are used, such as DNS over TLS, DNS Over HTTPS, alternative DNS resolvers or VPNs. Filtering is disproportional and can have an impact on innocent people that use the same infrastructure; it also has an impact on Internet performance, and generates distrust among the users (see AFNIC-.FR ccTLD report). Filtering at the DNS level can be extremely untransparent and create many governance issues. The AFNIC report asserts that it could actually affect access to a global, open Internet and fragment it, creating inconsistencies in how users experience the Internet.

Despite the hesitations of the technical community and numerous advocacy initiatives by digital rights organizations, regulatory initiatives around the world increasingly lean towards blocking at the DNS level as well as directly ordering DNS resolvers to block websites.

Usually the blocking orders are not detailed and are not prescriptive. (Mentioned in an interview with Douglas Fischer.) In other words, the orders might not even mention that the ISPs should block the domain name at the DNS level. But some argue that blocking at the DNS level is ISPs go-to solution as it is more efficient and less costly. Liquid, a network operator in Africa mentioned during our interview, said:

"So you can generally, we have a regulatory requirement in certain countries to filter specific websites, block specific websites. [...]but there are two technical ways to achieve that. One, you can do full scale Deep Packet Inspection, possible SSL inspection, if you've got the capacity or the ability to do so, which is SSL interception is a different story for a different day, because you can't realistically do that at the carrier level. But you either do it at the DPI level, where you're inspecting SNI, IPS, and you can do the blocking. It's quite intensive, quite expensive, and not reliable or *you can do the DNS where you can block a DNS lookup*."

- **What are the alternatives to blocking? No rendez vous disrupted**

As mentioned previously, the technical community has clearly pointed out why blocking at the DNS level does not always align with the Internet architecture. In RFC 7754, they mention that it is better to inform the end-points of the potential illegal or malicious content and service instead of blocking and disrupting the rendezvous. Endpoints include a client and a service. They can be a browser or a content host.

What is a rendezvous? According to RFC 7754 Rendezvous services are service endpoints that are typically identified by identifiers that are more "human-friendly" than IP addresses. Rendezvous services allow one endpoint to figure out how to contact another endpoint based on an identifier. An example of a rendezvous service is the domain name system. Distributed Hash Tables (DHTs) have also been used as rendezvous services." If we adopt a no rendezvous disrupted approach, then we need to have alternatives to blocking. A few alternatives include:

- Browser-Based Security: Security measures can be implemented in web browsers to warn users about malicious websites.
- Content Filtering at the User Level: Providing tools that allow users to filter content at the home network level may be more appropriate

than blocking at the DNS level

- **Open source software and DNS resolvers**

Open source software was one of the fundamental bases of growth of the Internet. The definition is always disputed and used in different contexts to mean different things, but one of the most interesting "open source" definitions is that open source is a bill of rights for computer and Internet users.[1] (Perens, 2009) Open source software and programming makes sure the rights to copying, distributing, access to source code and the right to make improvements to the program are maintained. Open source software is important for creating competition and combatting monopolization of the market; however, they might face the tragedy of the commons (Hardin's theory). If open source software initiatives do not have the institutional design that allows their growth, then they will fade away over time and will be replaced by commercial ventures that might have used those very open source softwares. (See Schweik, Charles M., and Robert English. 2007.) [2]In this research, we have not methodically assessed whether tragedy of the commons happens in open source DNS resolvers. However, there were some interesting insights in the interviews about the use of open source software in providing DNS resolvers:

The interviewed DNS operators did not express grave concerns about using open source software to run their resolvers. One ISP explained that they mainly use commercial recursive resolvers for customer resolution, because this is what they have been doing since the beginning of operating their ISP. (Comcast) It was added that they use open source software in their other resolvers, particularly in their enterprise network to support employee resolution, and they do not have concerns regarding the use of open source DNS resolvers. However, they did note that it was challenging to find an open source DNS resolver software that could operate at a very large ISP scale (over 1.8 billion queries per day). They require a specific response time and a team of experts who could troubleshoot.

OpenDNS mentioned that they liberally use open source software for their DNS resolvers, but there are some services offered to businesses that

[1] Bruce Perens, "The Open Source Definition," Open Sources: Voices from the Open Source Revolution, January 1999.
[2] Charles M. Schweik, Robert English, Tragedy of the FOSS Commons? Investigating the Institutional Designs of Free/Libre and Open Source Software Projects." First Monday 12 (2). https://doi.org/10.5210/fm.v12i2.1619

cannot be open source and should not be shared for security reasons.

DNS4All, which is an experimental DNS resolver provider, mentioned that they have full trust in open source software and especially in those softwares they have chosen. They gathered trust through past experiences and the use of open source software.

Considering that there was not much hesitation from the network operators and DNS providers to use open source software, we wondered why there are not many popula nonprofit DNS resolver providers other than Quad 9 and a few others that ISPs and other network operators could use. So we asked the Internet Society why they do not run a DNS resolver (Internet Society is a not for profit organization that advocates for meaningful connectivity). The response was that their mission does not include providing Internet infrastructure, but they work on enabling other actors to provide Internet infrastructure and they would recommend using open source DNS infrastructure.

Then, based on the hypothesis that perhaps other not for profit organizations that provide Internet infrastructure (such as Country Code Top Level Domains) might find it easier to provide other DNS services, such as DNS resolvers, we asked a few ccTLDs why they do or do not provide DNS resolvers. They responded that providing DNS resolvers would open the door for more liability and as infrastructure providers they did not want to get involved with content regulation. The emergence of regulations around such as the EU's Network and Information Systems Directive 2 that requires excessive security measures and other practices also does not incentivize the ccTLDs to provide additional services.

All in all, it does not seem like open source DNS resolvers are unreliable or actors are reluctant to adopt them. The reason for not providing open source DNS resolvers for free lies elsewhere: heavy regulation, lack of economic incentives, lack of capacity in some instances and lack of a mandate to provide infrastructure.

- **Maintenance of the DNS Resolver services**

One of the recurring themes about why Internet Service Providers use public resolvers and do not provide their own was the cost and maintenance of the resolvers and also size and geographic location of the ISP. For example, an ISP based in Switzerland might not mind using a public DNS resolver and a Content Delivery Network based in Germany because the difference in speed and latency between a local cache and DNS resolver and an international one might not be very significant. However, in large countries such as the US, having a local cache and DNS resolver is pivotal for providing meaningful connectivity, due to CDN-based content localization where dynamic authoritative responses direct users to the most local, directly peered routes (Interview with Comcast). Based on one of the interviewee's opinions, provision of DNS resolvers by the ISP is the most basic service that an ISP should provide to its customers. (Comcast)

Providing meaningful access to content and online services, however, goes beyond just resolving DNS queries and maintaining a well functioning DNS Resolver that can be used anywhere around the world needs investment in infrastructure. For example, CIRA utilizes multiple DNS servers, routers, and switches to ensure reliability. They have connectivity to the Internet through transit providers and local Internet exchanges. CIRA owns a rack in the buildings where the Internet exchanges are located, rather than relying on free space or power from the exchanges. They have more than a dozen servers in eight locations across Canada. The infrastructure is designed to support all 33 million Canadians. Quad9 undertakes several measures to maintain its DNS resolver service, focusing on reliability, security, and performance. It also has a specific approach to Internet Exchange Points (IXPs). The following is a breakdown of their maintenance and IXP strategies based on the interviews:

- Multiple Server Locations: Quad9 has over 230 locations worldwide, with the aim to push servers as close to the edge of the network as possible. This global distribution helps ensure that users are served by a nearby server, improving speed and reducing latency.
- Anycast Network: They use anycast to route traffic to the nearest available server. This ensures high availability and reduces the impact of server failures. If one server goes down, another one takes over.
- Software Diversity: Quad9 uses a mix of open source software, including Unbound, PowerDNS, and BIND. This diversity helps them avoid reliance on a single software platform, reducing the risk of service disruptions. They use DNSdist as a front-end. They update their systems regularly.

- The Startup Hypothesis

Another obstacle that could hamper ISPs and network operators' ability to provide and maintain DNS resolvers is the size of the ISP. When ISPs are at a startup stage, they might have difficulties providing their own DNS resolvers. Some ISPs also might not want to provide DNS resolvers services, not to be inundated by the government's request for blocking websites. When we discussed this with a network engineer from Brazil, the startup theory was also brought up. The discussion took us in a different direction: it might not actually matter where the ISP is located, since small and mid-size ISPs might not be able to maintain an important piece of infrastructure. This might take the research in another direction: instead of focusing on regions and countries, we might want to analyze the ISPs and other network operators' incentives to provide their own resolvers based on their size and the service they provide.

Incentives and deterrents to adopt public DNS resolvers

One of the questions that the research addresses is: why would ISPs and other network operators use public DNS resolvers as opposed to providing their own DNS resolvers or using their ISPs? We loosely applied the theory of "make or buy" by Williamson to this question. Williamson was a prominent economist that developed the Transaction Costs Economics of "make or buy". He came up with a scheme that identifies under what circumstances a firm decides to outsource or make the product. Williamson asserted that such decisions depended on a few variables: search and information costs, bargaining and decision costs, governance complexities, asset specificity (the more the asset is generalized and not specific the less the transaction cost of providing it), uncertainty (the sources of disturbances to which adaptation is required), and frequency, which means reputation effects and setup costs.[3]

Another factor that should be considered when assessing the incentives and deterrents of adopting public DNS resolvers is the kind of network operator. Not all network operators are Internet Service Providers, they could be cloud services, hospitals, government agencies and they have different incentives and deterrents to provide or outsource the DNS resolver function.

Search and information costs: Using public DNS resolvers does not involve much search and information cost, especially if the network operators choose the dominant and well known public resolvers that are well established in the market. This might be one of the reasons that network

[3] Williamson, O. E. (2008). Outsourcing: Transaction cost economics and supply chain management. Journal of Supply Chain Management, 44(2), 5–16)

operators opt for Google Public DNS and Cloudflare (according to APNIC Lab data) rather than other public resolvers. Bigger and more well established public DNS resolvers can provide more information about their service's security and other processes more easily so it reduces the transaction costs for the network operators. One of the reasons that smaller public resolvers can also become popular (like Quad9, which has 228 pops around the world) is providing such information to the network operators and peers with Internet Exchange points and others which can ultimately bring down the search costs and the information costs for the network operators.

Bargaining and decision costs: Some of the public DNS resolvers do not even have a Service Level Agreement or do not need to receive one from the public resolvers (See Google's public DNS resolver policy) so there might not be much in the way of bargaining for some ISPs, especially if they are smaller.

Uncertainty and frequency: Williamson also considers uncertainty and frequency as two elements of transaction costs. When applying uncertainty and frequency to DNS resolvers, we can identify a few factors. For example, the DNS resolver provider (the network operator including the ISPs) has to maintain the stability and security of the public DNS resolver which can be costly and resource intensive. The frequency, which includes reputation and set up costs, can also increase the transaction costs of providing a local public DNS resolver, especially when more cost effective alternatives exist. As one of the interviewees from Digital Economy Advisors (and former CTO of Liquid) said: "If you're a small ISP and you've only got one guy or two guys, and then he leaves, or she leaves, you can find yourselves always struggling with skill. There is a certain skill needed to maintain this thing." Liquid also added that smaller ISPs and network operators often have difficulty maintaining reliable DNS resolvers due to limited resources, staff turnover, and a lack of technical expertise.

Governance: Governance of DNS resolvers similar to technical matters is becoming more and more complex, increasing transaction costs. If we consider third party public resolvers are competing in a competitive market, then users and operators select these services based on factors such as performance (lack of latency), security, privacy, lack of censorship and costs. But the expectation and the demands of an individual user and even a small ISP might be different than the demands of large telecom operators that have many clients or network operators that have clients with specific security needs (such as government agencies).

When ISPs and network operators start providing their own DNS resolvers, it will require a hierarchical governance which is more costly and less adaptive. They need to comply with laws and regulations and keep their compliance current. Governance is one of the reasons why network operators might use third party public resolvers. During the interviews we asked the interviewees why they or their customers would use public DNS resolvers. Quad9 and Whalebone responded that because of the security services they provide, their customers (especially when they are not well sourced network operators) often prefer to use their services instead of providing their own resolvers. Whalebone also mentioned that complying with all the regulatory requirements might not be feasible for a small ISP or an enterprise, so for legal compliance they also use Whalebone compliance services. In one of our interviews with a Bangladeshi ISP, it was mentioned that they considered using 1.1.1.1 (Cloudflare filtered DNS resolver) in the resolver pool to comply with the Government's interim directions to filter adult porn sites. They mentioned that at the moment, however, they have not received any blocking directions.

Hybrid governance happens when a government starts partnerships with the private sector to provide DNS resolvers. The EU's DNS4EU project can fit the description quite well. This kind of governance mechanism might change the incentives for different network operators to provide their own resolvers or just use services like DNS4EU as those services could potentially lower the costs of operation in general.

Why would end users switch to public DNS resolvers?

The evidence that could give us an understanding of the incentives for end users to switch to public DNS resolvers is of anecdotal value for the moment.

Good Enough! Some of our interviewees mentioned that it is possible that public DNS resolver providers' advocacy to use their DNS resolvers instead of their ISPs might have actually worked on some populations. Liquid, for example, mentioned that in regions like Africa, global public resolvers historically lacked local and optimal DNS infrastructure, but in some cases even the ISPs recommended their users to switch to public DNS resolvers. Liquid mentioned:" Call center staff, I kid you not, would actually recommend switching off from our DNS at the time to Google DNS, despite it being inferior." But the use of public DNS resolvers is not uncommon as a back-up plan.

The Bangladeshi ISP, for example, said that sometimes customer service suggests the customers to use Quad8 (Google) or Quad1 (Cloudflare) but this is always a decision that the customer can make for themselves and they emphasized that they do not reconfigure it. Alternatively, the DNS resolvers like Quad9 can partner with ISPs, IXPs and other network operators and provide a streamlined service that individual users use. As John Todd from Quad9 mentioned: "We have multiple partners who give us network infrastructure at no cost. And again, this is the benefit of being a nonprofit that's doing good. Network providers are people who understand the infrastructure of the Internet. They want to see us succeed. And we're really happy that we have some great partners." CIRA also mentioned that individual users can start using other DNS resolvers because of the partnership with other endpoint providers such as browsers. For example, CIRA has partnered with Mozilla to provide DNS resolver services for Canadians.

A Matter of Trust: Another reason that individual users use public DNS resolvers is that they do not trust their ISPs DNS resolvers. Fischer (the Brazilian network engineer) mentioned that when the ISPs are ordered to block a large list of domain names without giving any reasons to the consumers whatsoever, that could erode trust in their ISPs and they might trust the public DNS resolvers more, hence resulting in a switch.

The IT professional effect: CIRA (the Canadian ccTLD operator that provides DNS resolvers) mentioned that their individual customers might use CIRA's DNS resolver because their tech-savvy network recommends it and sets it up. Anecdotally we hear that network operators and system admins that try to advise the users on how to circumvent censorship, change their personal computers DNS resolvers. We tried to establish whether there was a correlation between political events during which people might not trust their government and so seek using public DNS resolvers that cannot be censored. As we mention in the quantitative section of this report, we could see some spikes during political events in the use of public DNS resolvers in India and France.

People recognize centralized services better: Larger public resolvers that provide different products can also more easily be trusted by the user (because they know the name) and they can advertise their services when the user uses the public facing, less technical platform (for example they could advertise using GoogleDNS when the user is using the search engine). It is however worth mentioning that despite the fact that Google provides a web browser to its users, it does not by default provide GoogleDNS, and the user has to change the setting to use GoogleDNS. This might also be because GoogleDNS might not want many users to overwhelm its network as providing a DNS resolver is not in its core mission.

Smaller DNS resolvers do not have the capacity to publicize their services at a large scale, so those who are tech-savvy either find them and recommend them or move to other DNS resolver providers in case the large DNS resolver provider does not provide its service (for example, when OpenDNS stopped providing their services for France, the users moved to DNS4all experimental initiative).

Digital Sovereignty and Internet Fragmentation

The trend of digital sovereignty and assertion of digital sovereignty also fuels blocking and filtering at the infrastructure level and it specifically affects the DNS. The attempts to territorialize the Internet can be done more efficiently and easily through Internet infrastructure. There are many debates on what digital sovereignty is and scholars have been working on it for years. (see Pohle, J., & Thiel, T. (2020).[4] This report does not delve into those debates; however, one kind of digital sovereignty that has been identified is when Nation States try to exert control over the flow of information in their borders. Mueller calls this alignment. Asserting real national sovereignty is not possible without fragmenting the Internet.[5] Usually nation states that are of a more democratic nature try not to exert digital sovereignty through Internet infrastructure that could lead to its fragmentation. However, it is important to note that it has become very difficult to define the Internet's core services and digital infrastructure, and some jurisdictions recognize DNS resolvers as essential services and digital infrastructure and do not necessarily exempt infrastructure from liability. As we will explain, even when a safety law exempts these services from liability, some responsibilities can remain.

[4] see Pohle, J., & Thiel, T. (2020) Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532

[5] Read generally Milton Mueller, Will the Internet fragment?,Mueller, M. (2017). Will the Internet fragment? Sovereignty, globalization and cyberspace. Polity Press.

- Digital Services Act and DNS resolvers

The Digital Services Act is an online safety law that the EU enacted which has been very focused on social media platforms. The EU decided that the Digital Services Act applies to DNS services, however clarified in recital 29 that DNS services and resolvers are intermediary services which exempt them from liability; but in recital 27 it emphasizes that: "Whilst the rules on liability of providers of intermediary services set out in this Regulation concentrate on the exemption from liability of providers of intermediary services, it is important to recall that, despite the generally important role played by such providers, the problem of illegal content and activities online should not be dealt with by solely focusing on their liability and responsibilities."[6] In recital 34 it lays out how the exemption does not apply to all EU jurisdictions and individual nation states can request blocking of illegal content, more specifically the recital ends with: "Those conditions and requirements should not affect the possibility for Member States to require a provider of intermediary services to prevent an infringement, in compliance with Union law including this Regulation, and in particular with the prohibition of general monitoring obligations." and finally in Article 10, 11 and 13 it requires all intermediary services (including DNS service providers) to provide their rules for content moderation in their terms and conditions, publish annual transparency reports and designate a point of contact for member states to reach out to. Doing transparency reports and being open about content moderation is one of the most fundamental steps that DNS resolvers can take. However, the fact that the EU does not consider an exemption for DNS services and DNS resolvers can create a fragmented approach to domain blocking at the DNS level and lawsuits can be filed in jurisdictions that require DNS resolver blocking which will have EU and global wide effect.

- Network and Information Security (NIS2)[7]

NIS2 is an EU directive that was enacted in 2022. While it is not necessarily about domain name blocking, and it is presented as a solely security

[6] Recital 29 of the European Union's Digital Services Act (DSA) considers DNS resolvers as mere conduit services "Whether a specific service constitutes a 'mere conduit', 'caching' or 'hosting' service depends solely on its technical functionalities, which might evolve in time, and should be assessed on a case-by-case basis."

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

related directive, it applies to DNS resolvers. Annex I section 8 of the directive considers DNS resolvers as Digital Infrastructure.

- Social media, tech companies governance and DNS resolvers

Nation-states sometimes employ DNS blocking to compel technology companies to engage in content moderation. For instance, the Malaysian Communications and Multimedia Commission (MCMC) recently took steps to restrict the use of public DNS resolvers. In a statement, the MCMC mentioned collaborating with local service providers to enhance prevention and protection measures, particularly in Domain Name System management. The commission cited its authority under the Communications and Multimedia Act 1998 to block access to websites violating Malaysian law, aiming to "protect the people, especially those vulnerable to online harm." This development is significant because governments are leveraging DNS resolvers to pressure social media platforms and messaging apps into obtaining licenses to operate within their countries to obtain licenses to provide their services inside a country.

In 2024, when X decided not to follow the supreme court order in Brazil that related to content moderation policy and privacy of Brazilian users, the supreme court ordered Anatel to operationalize the blocking of X in Brazil. Anatel is the Brazilian regulatory authority which hands in the orders to different ISPs. When receiving blocking orders, ISPs usually block the domain name through DNS resolvers. There are usually no guidelines and no nuanced instructions on how to do it, which can have an impact on users' access and erosion of trust in the user. In this case there was no specific ruling that obliged DNS resolver operators to block X; however, these kinds of actions could also put DNS resolvers at risk, especially after X decided to run the platform for Brazil on Cloudflare, Fastly and Edgeuno. (Guardian, 2024)

Quantitative Data analysis

Our data analysis has addressed the following questions:

1) Is there a trend in using public DNS resolvers instead of ISP provided DNS resolvers around the world?
2) Was there any correlation between Internet freedom and using DNS public resolvers?
3) Was there any correlation between the country's GDP and use of public resolver?

We asked these questions to understand whether DNS public resolvers are becoming more popular, and if they are, why they are becoming more popular and if the Internet Service Providers provided local DNS resolvers, whether this was to undertake censorship and blocking.

Source of Data; APNIC DNS Resolver Use

For this research we have used APNIC Labs DNS Resolver data to understand the public DNS resolver use around the world and identify the trends. We did look into other sources of data to understand the adoption of DNS public resolvers, but as we explain in the section on sourcing data, APNIC Lab's data so far was the most appropriate for the research.

Understanding APNIC's data

APNIC Labs end user statistics determine the resolver in use by end users throughout the world. Their test purchases advertisements through Google and instead of sending an advertisement, sends a single blank pixel with a unique URL per user per visit. Through that unique URL, APNIC is able to capture a large amount of information about the end user who viewed the advertisements, including their origin autonomous system and the DNS resolver they used to resolve the requests related to the advertisement served.

APNIC data limitation

There are some data limitations in APNIC data. For example, different ISPs can have different internal resolver architectures, and it will only be visible to the last member of that architecture. The users being served with the APNIC advertisements are subject to a credit limit per day, with no uniformity during the time of the day. A user visiting a site that does not use Google Ads is unlikely to be measured. There is also a potential bias where Ad serving focuses on richer economies, under-representing less affluent populations.

Is there a trend in using public DNS resolvers by ISPs worldwide?

The question on whether there is a trend in using public DNS resolvers globally by ISPs based on the data analysis we have undertaken has to be answered in a more nuanced way.

We have looked at the data between June 2022 and June 2024. We analyzed the use of public DNS resolvers as opposed to ISP resolvers for each region. APNIC Lab regional and sub-regional divisions align with UN Statistical Division regional groups.

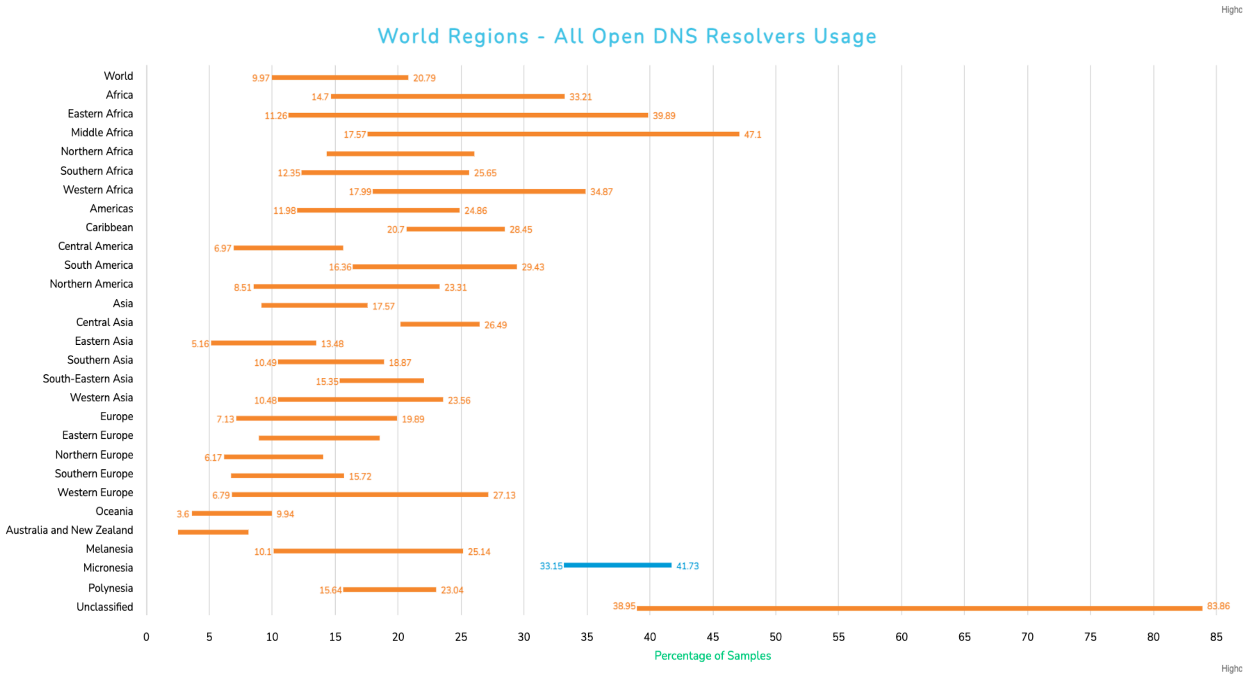
Globally, the use of DNS resolvers by the ISPs has not become popular from what we see in the data, and in fact the use of public DNS resolvers have gone down. This trend, however, changes when we look at the data in sub-regions or depending on who the network operator is. You can find the raw data on our GitHub repository.

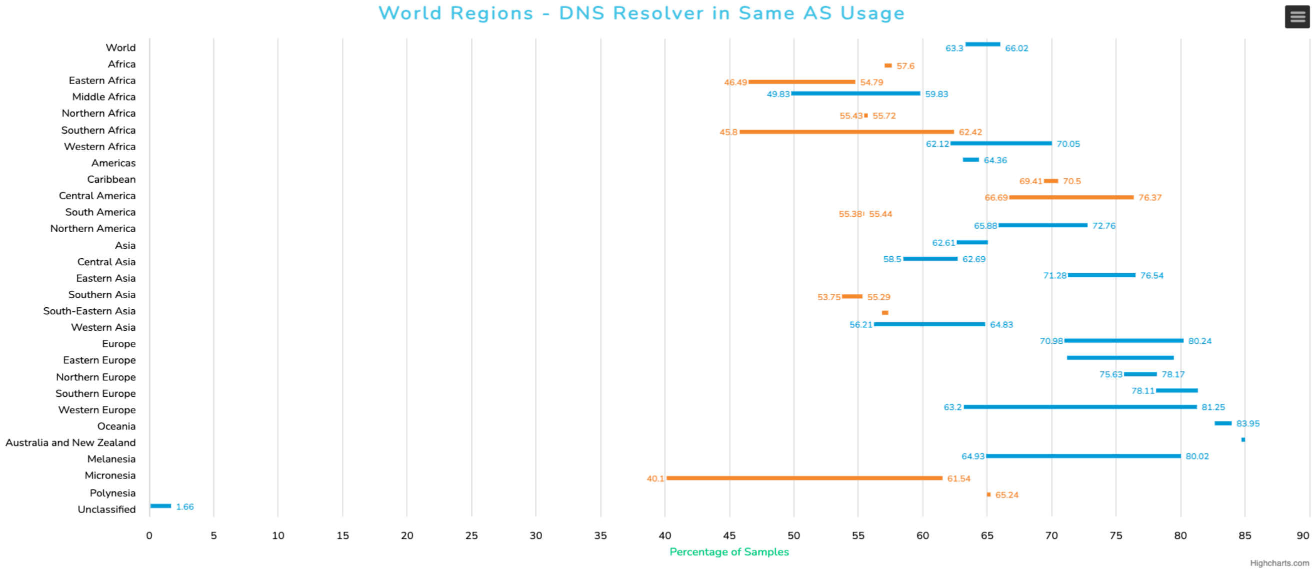
Plots

The plots below compare the usage of public DNS resolvers and local DNS resolvers between June 2022 and June 2024. If a bar is blue, it means usage increased between 2022 and 2024. If a bar is orange, it means the usage of the public or local DNS resolver has decreased between 2022 and 2024. The length of the bar shows the usage change.

The plot on DNS Resolver in Same AS Usage, describes how many of the samples were served by a DNS resolver in the same ASN. This indicates using a local resolver.

All Open Resolvers Usage, describes how many of the samples were using an Open Resolver. APNIC is currently tracking 29 open resolvers.


Highc
World Regions - All Open DNS Resolvers Usage
World
Africa
Eastern Africa
Middle Africa
Northern Africa
Southern Africa
Western Africa
Americas
Caribbean
Central America
South America
Northern America
Asia
Central Asia
Eastern Asia
Southern Asia
South-Eastern Asia
Western Asia
Europe
Eastern Europe
Northern Europe
Southern Europe
Western Europe
Oceania
Australia and New Zealand
Melanesia
Micronesia
Polynesia
Unclassified
9.97
20.79
14.7
33.21
11.26
39.89
17.57
47.1
12.35
25.65
17.99
34.87
11.98
24.86
20.7
28.45
6.97
16.36
29.43
8.51
23.31
17.57
26.49
5.16
13.48
10.49
18.87
15.35
10.48
23.56
7.13
19.89
6.17
15.72
6.79
27.13
3.6
9.94
10.1
25.14
33.15
41.73
15.64
23.04
38.95
83.86
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
Percentage of Samples
Highc


World Regions - DNS Resolver in Same AS Usage
World
Africa
Eastern Africa
Middle Africa
Northern Africa
Southern Africa
Western Africa
Americas
Caribbean
Central America
South America
Northern America
Asia
Central Asia
Eastern Asia
Southern Asia
South-Eastern Asia
Western Asia
Europe
Eastern Europe
Northern Europe
Southern Europe
Western Europe
Oceania
Australia and New Zealand
Melanesia
Micronesia
Polynesia
Unclassified
63.3
66.02
57.6
46.49
54.79
49.83
59.83
55.43
55.72
45.8
62.42
62.12
70.05
64.36
69.41
70.5
66.69
76.37
55.38
55.44
65.88
72.76
62.61
58.5
62.69
71.28
76.54
53.75
55.29
56.21
64.83
70.98
80.24
75.63
78.17
78.11
63.2
81.25
83.95
64.93
80.02
40.1
61.54
65.24
1.66
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
Percentage of Samples
Highcharts.com

Correlation between Internet and press freedom and the use of Public DNS resolvers.

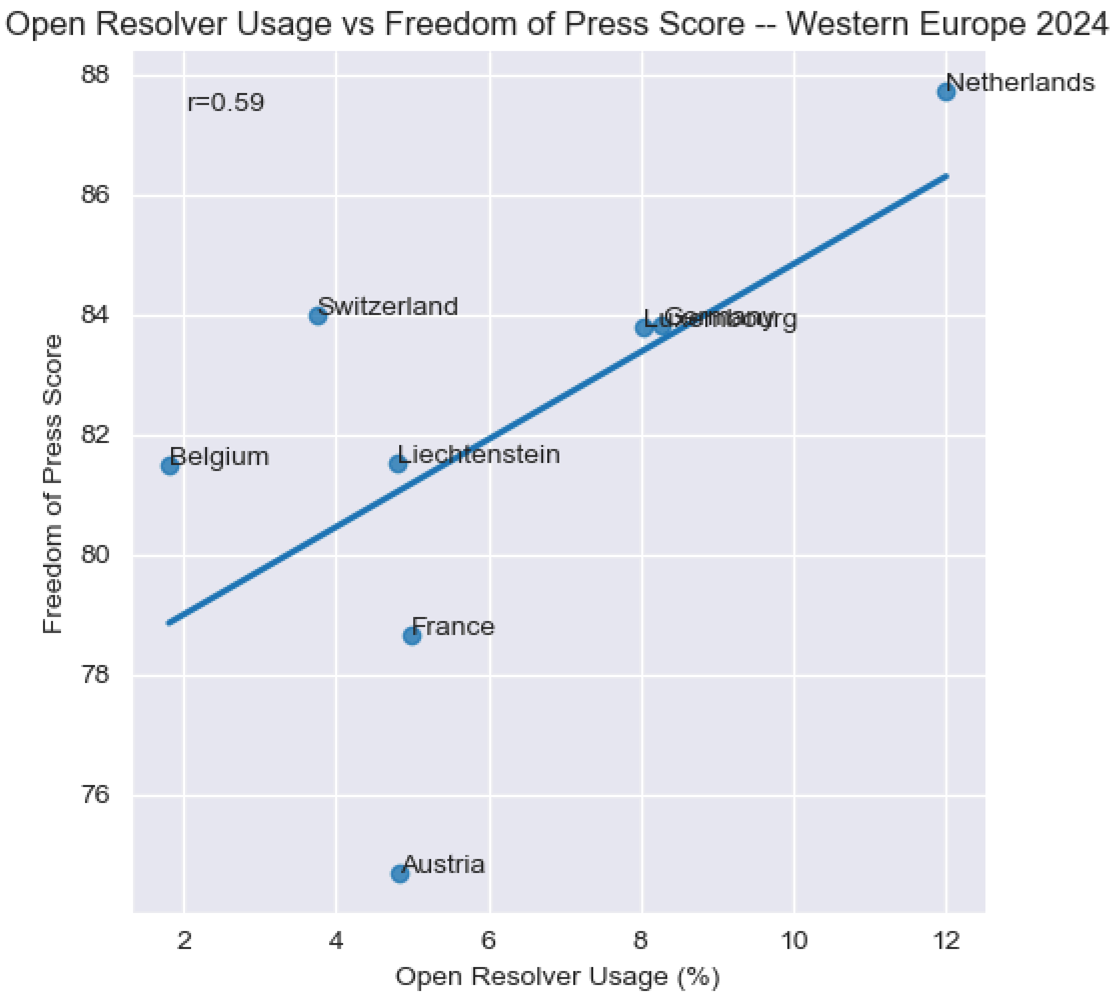
Globally, there was no meaningful correlation between Internet freedom and the use of public resolvers, with a correlation coefficient of -0.12. The data point we considered was in June 2024 for each country, against the Freedom House Internet freedom index in the same year, and calculated the correlation for countries within sub-regions. We did the same with the Press Freedom index. Also in the indices some countries were missing and were not covered (for example, Tajikistan's Internet freedom has not been ranked in Freedom House's index).

While at a global scale we did not see a meaningful correlation between Internet freedom and the use of public DNS resolvers, we saw some correlation when we looked at some of the sub regions.

Sub-regions and Press Freedom

- Western Europe and Press Freedom

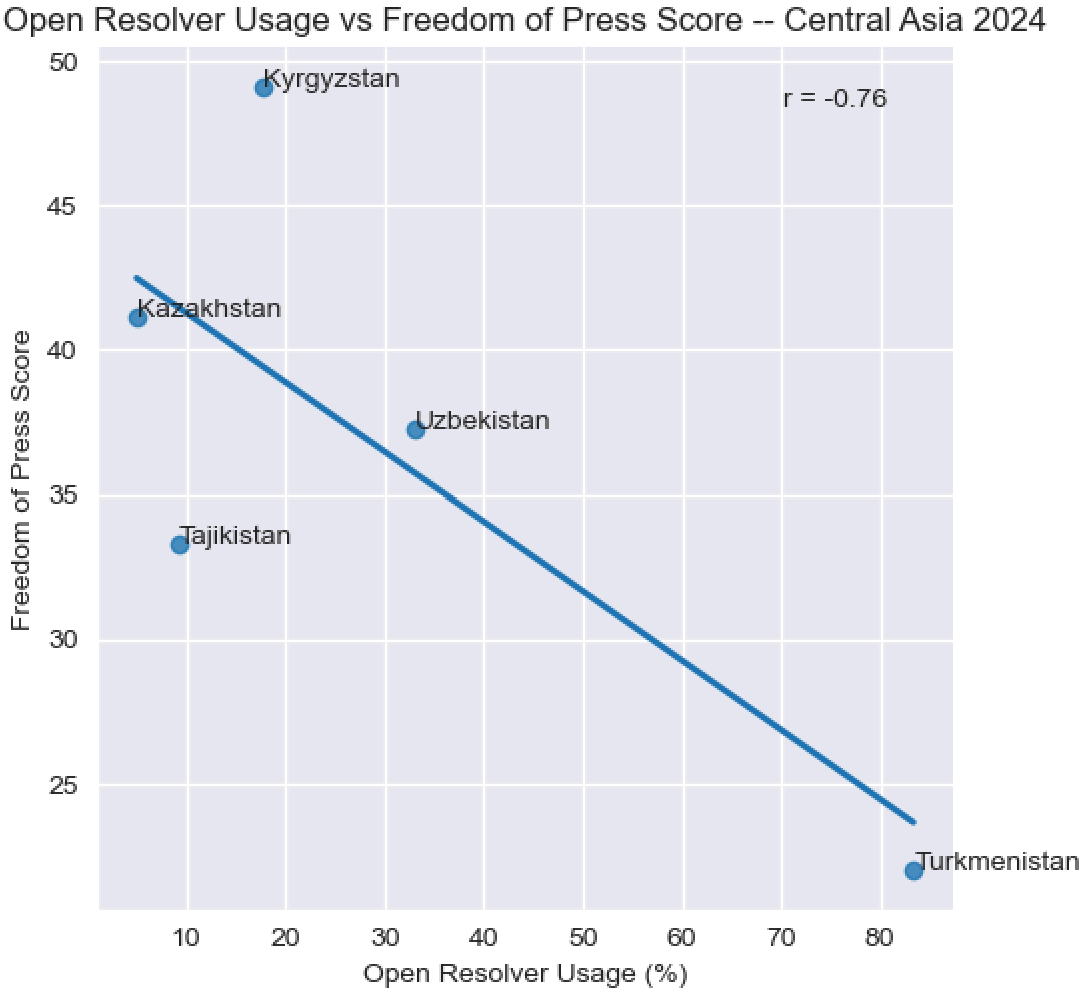
There was a positive weak correlation between usage of public resolvers and Press Freedom Score, in Western Europe. This means higher usage of Public Resolver where the press Freedom Score is higher. Western Europe included France, Germany, Netherlands, Belgium, Austria, Switzerland, Luxembourg, Monaco and Liechtenstein.



Analysis of this data: https://stats.labs.apnic.net/rvrs/QO?o=cXEw1l1s0t10x

Central Asia and Press Freedom

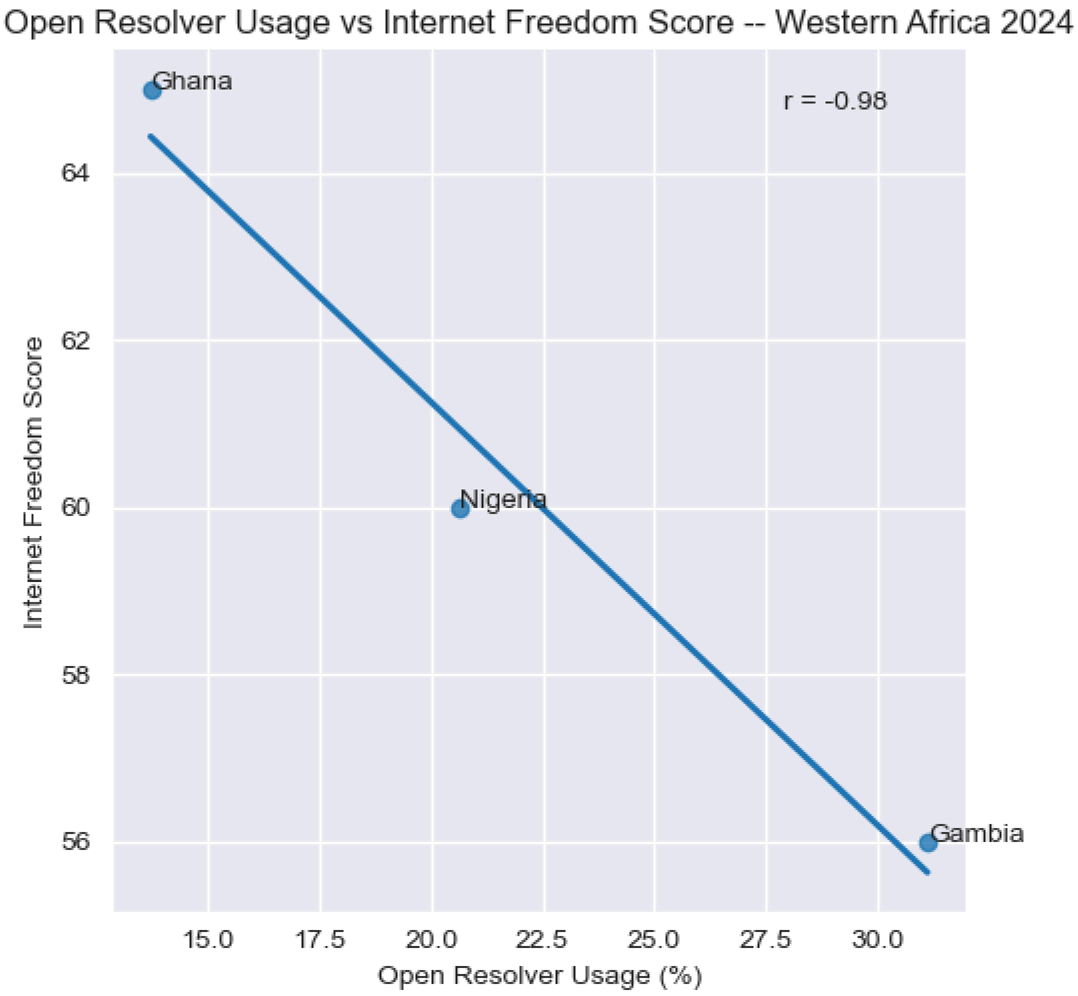
There was a negative correlation between usage of public resolvers and Press Freedom Score, in Central Asia. This means that the lower press freedom score was, the use of public resolvers was more popular.



Data Source Analysis: APNIC Lab stats: https://stats.labs.apnic.net/rvrs/XR?o=cXAw1l1s0t10x

Western Africa and Internet Freedom

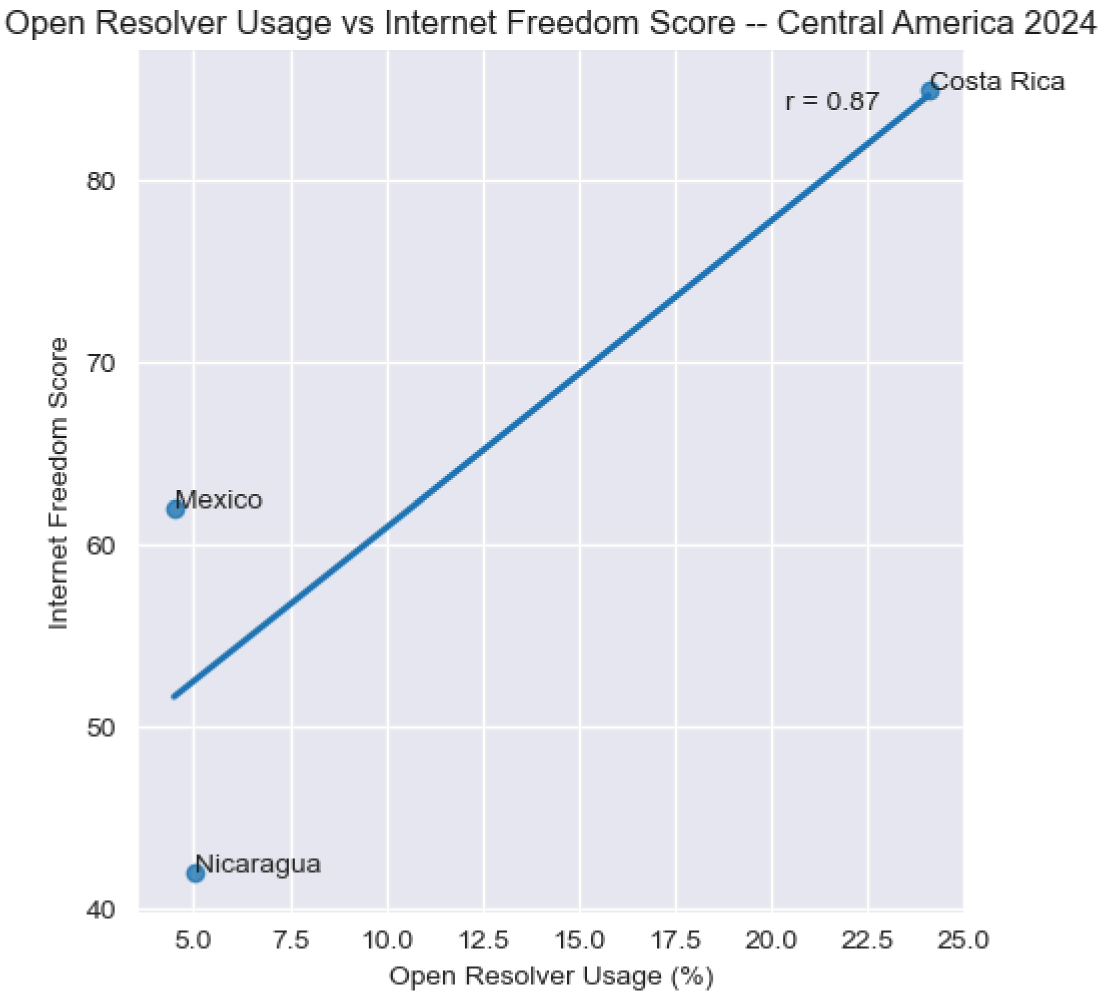
There was a negative correlation between Internet freedom index and usage of public resolvers in Western Africa. Where there was lower Internet freedom, there was a higher usage of public resolvers.



Source: APNIC https://stats.labs.apnic.net/rvrs/XL?o=cXAw1l1s0t10x

Central America and Internet Freedom

There was a positive correlation in Central America, more Internet freedom aligns with more public resolvers usage.



Was there any correlation between the country's GDP and use of public resolver?

During our interviews and desk research, we came across the argument that some ISPs in developing countries do not provide their own DNS resolvers and rely on Google and Cloudflare because it is too expensive to provide and maintain DNS resolvers. From transaction cost economics we also learned that firms usually try to externalize the costs when they cannot internalize it due to various reasons, such as technical skills, operational matters and others. To test this argument with our data, we looked at a country's GDP and the use of public resolvers. We obtained the countries' GDP from the World Bank. It is worth noting that the World Bank's data is only available until 2023.

The data did not reveal any meaningful correlation. We also looked at the size and population of a country, especially Small Island States. There didn't exist a meaningful correlation in Small Island States either (Fiji for example is a small island state but the use of public resolvers is not that popular). The charts below illustrate the top 10 countries in APNIC data that use public DNS resolvers the most and the bottom 10 countries that have the lowest usage of public DNS resolvers the least:

Countries with the lowest public resolver usage:

cc_name	Average Open Resolver Usage	Average Number of Samples
Nauru	0	12
French Guiana	0.56	177
Fiji	0.76	1983
Guernsey	0.84	835
Yemen	1.08	8035
Kuwait	1.3	19495
Mongolia	1.35	7243
Republic of Korea	1.77	124700
Angola	1.82	10796
Cote d'Ivoire	1.9	21949

Countries with high usage of public resolvers

Country Name	Average Open Resolver Usage	Average Number of Samples per day
Brunei Darussalam	90.13	1489
Saint Pierre and Miquelon	86.36	66
Kiribati	83.87	62
Wallis and Futuna Islands	83.33	12
Sierra Leone	77.45	7415
Northern Mariana Islands	76.78	267
Timor-Leste	72.32	336
Central African Republic	71.21	132
Chad	69.6	1283
Haiti	66.13	7549

While we have seen through the data that the use of DNS resolvers in particular regions, such as Africa, might have increased in the past, this trend appears to be on the decline (however not in all countries). To understand the data better we decided to focus on a few countries that either had a high adoption rate of public DNS resolvers (for example Liberia) or countries that based on APNIC's data had a significant decline in the use of DNS public resolvers. As mentioned above, it might also be that we need to introduce another unit of analysis instead of emphasizing regions and countries. The size of the ISP and the nature of the business as well as whether there is diversity of local ISPs or whether the country is dealing with a telecom operator monopoly might be the deciding factor in providing DNS resolvers or using public resolvers, and not necessarily the region or the country.

This however does not mean that GDP is not related to the use of DNS public resolvers, but the explanation for adoption of third party public resolvers might not just be lack of skills or financial resources. This is why we interviewed prominent telecom operators in Africa to understand the reasons.

Reasons for Decreased Adoption of Public Resolvers in Africa

In Africa, we noticed a difference and decrease in the use of public DNS resolvers. There is an interesting story behind the use of public DNS resolvers in Africa. It seems that unlike the general perceptions that users do not know much about public DNS resolvers, for quite awhile since the Internet Service Providers DNS resolvers were not operating well, the users opted for using public DNS resolvers. However, public DNS resolvers did not work that efficiently either as they did not cover most countries in Africa. Users experienced reliability problems when using public resolvers located off the African continent. This could result in higher latency and slower performance, leading to dissatisfaction and reduced usage. But compared to their own ISP, the public resolvers were doing better(Interview with Liquid).

An interesting movement started happening around 2015 in Africa. Internet Service Providers increasingly started receiving complaints from their consumers that their Internet does not work (this meant that their DNS resolver did not resolve the queries, otherwise the consumers were online and infrastructure wise everything worked). In a 2018 report published in CAIDA by Fanu et al, the DNS configuration was identified as one of the major connectivity hurdles and that ISPs even by default used third party public resolvers. Internet Service Providers (especially Liquid) decided to invest in optimizing their DNS resolver services so that the consumers do not use public DNS resolvers that did not have a strong presence in Africa. In 2015, Liquid migrated its customers to the Anycast Domain Name System. Arguing in support of this important migration, it explained that the move adds to the resiliency and reliability of its users and clients connection and access to online services and content:

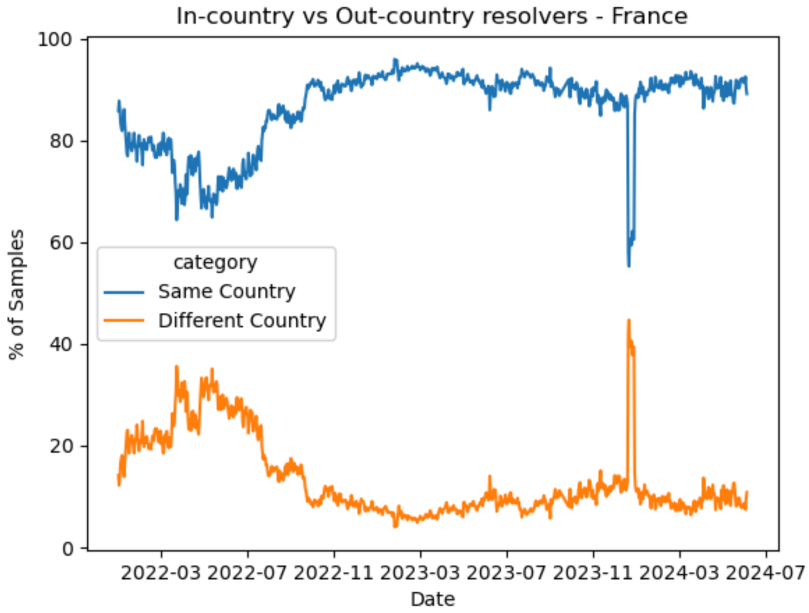
"Some ISPs use the Unicast DNS platform running on one server, sometimes with a single backup unit, to convert the website names into IP addresses so that users can access those sites, which could be on a server anywhere in the world. In the event of a natural disaster, power outage, sabotage or data fraud, servers using the Unicast DNS can go down, or in the case of heavy user traffic, there can be a long queue of requests. All of these factors can lead to downtime that is noticeable for Internet users. The Anycast DNS platform uses multiple servers to route the conversion of website names into IP addresses and automatically switches users to the closest functional server without any interruption."

Anycast DNS was also offered as an alternative to Google Public DNS in 2015 and at the time it was announced that it will be rolled out to countries such as Tanzania and Malawi. This is not to say that the use of public DNS resolvers is not popular in Africa anymore. In some countries like Gambia, even the main telecom operator (Gamtel) DNS traffic is handled by DNS public resolvers (especially Google). However, there has been a noticeable decrease based on APNIC data. The decrease might be attributed to investment in local DNS infrastructure and also the fact that public DNS resolvers such as Google services for Africa are sub-optimal and slow compared to ISPs own public DNS resolvers. (Fanou et al, 2018, page 18.)

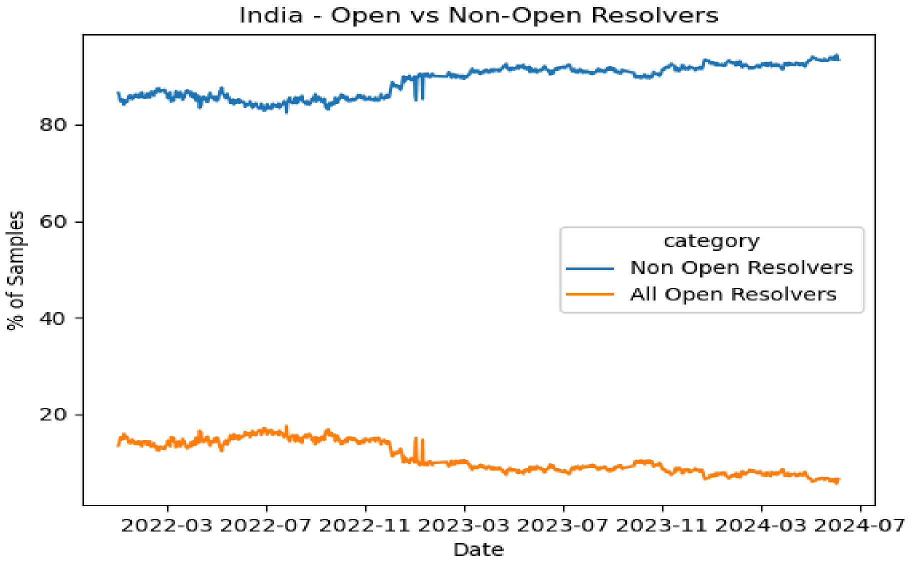
Some trends in individual countries:

Although we did not see a major correlation between the use of public DNS resolvers and Internet freedom globally and regionally, we identified some correlation regionally. We also identified spikes in the use of public resolvers when there was civil unrest or presidential elections. This does not only apply to undemocratic countries. One of the first of these cases (the use of non-ISP DNS resolvers) happened in 2008 in Turkey. The data that we have from APNIC (which tracks the use of public DNS resolvers between 2022 and 2024) shows another interesting trend in France and India. Future research could use our method to investigate whether these spikes can be seen surrounding other events in different countries. There has to be some control for cyber incidents and other issues that might have happened during those years that we see the surge in the use of public resolvers as well.

- In France, in 2024 there was a spike in the use of public DNS resolvers which coincided with the presidential elections. Interestingly, it also coincided with New Caledonia protest



- Spike in India in 2022: India saw several surges in public resolvers usage during 2022. This year also coincided with the elections.



Our method: A snapshot of the APNIC data for every country and region was collected in June 2024, tracking back to Jun 2022, with one data point per day. Each data point contains 53 columns describing how many of the measurements gathered from the specific country correspond to Open

Resolvers versus non-open resolvers, and which specific open resolver, plus other indicators.

To analyze India and France, we selected the data attributed to each country using their ISO3166-2 code (IN for India and FR for France), filtered out anomalous number of samples per day (the top and bottom 1%) and calculated the ratio of samples going to Open Resolvers vs non-open resolvers. This gives a good indication across time of the use of the likes of Google Public DNS and other large public resolvers.

Future Research

Our research used APNIC data to explore whether DNS resolver centralization is occurring. While we initially used “country” and “region” as our primary units of analysis, we found that these categories may not fully capture the complexity of resolver adoption trends. Network operators within the same region or country often differ significantly in size, structure, and incentives — making these geographic units less reliable for understanding underlying dynamics.

For instance, network operators in the same country might choose to use public DNS resolvers or offer their own for entirely different reasons. Regional classifications also fail to account for the diversity of motivations and infrastructure across operators. As such, future research could benefit from focusing more on the characteristics of individual network operators — such as their size, business model, and operational scope — to better understand the incentives and transaction costs that shape resolver choices.

One promising direction is to consider "informational borders" rather than strictly geographic ones. While country and regional policies remain relevant, more nuanced units of analysis — such as network type and operator category — may yield deeper insights. Future questions might include: Do satellite internet providers rely more heavily on public resolvers? How do cloud providers integrate DNS resolvers into their services, irrespective of geography?

A notable example is Starlink, where nearly 40% of DNS traffic is handled by Google and 58.1% by Cloudflare. Starlink openly talks about this in its policy but does not provide a reason why they use a public DNS resolver.[8] These patterns suggest that understanding DNS centralization requires a shift in focus — from regional mapping to examining how different types of networks interact with public resolver infrastructure.

In the future, it would be interesting to investigate why network operators other than ISPs rely on public DNS resolvers for their resolver needs instead of providing their own. Some of the answers were uncovered during our interviews with the DNS resolvers: Quad9 and Whalebone mentioned that their customers, especially enterprise customers, use their services because they provide security services. Some industries such as the health industry might also be heavily regulated and public DNS resolvers can provide them with a customized experience and lower the cost of compliance. John Todd from Quad9 in a panel discussion with the Cyber Peace Institute mentioned that while larger hospitals might be better at tackling malware and ransomware attacks, smaller healthcare providers, especially in rural areas, might not be that well equipped and public resolvers can help them. (See the panel discussion here)

Sourcing alternative data for the project

- Refining our method for analyzing APNIC data

Future research can refine our method for analyzing APNIC data, considering re-categorizing the regions to look into monitoring trends through adoption of DNS resolvers by different actors (size of the ISP, network operators business etc)

- Analyzing RIPE Atlas database

At present, as asserted by scholars and researchers, "the only publicly available dataset on user populations per ASN" is APNIC Lab data. We discussed and analyzed RIPE Atlas data at length with the help of Jim Cowie, a network engineer and historian. However, in the end, it became clear that for the purpose of our research RIPE ATLAS data might not be

[8] See Starlink "What IP Address Does Starlink Provide": In addition, when Starlink is in the process of connecting to the network, a default DNS server of 34.145.127.1 will be provided. Once the Starlink has verified connectivity with the Starlink network, then the DNS server will update to the DNS servers (usually 8.8.8.8 and 1.1.1.1).
https://www.starlink.com/support/article/1192f3ef-2a17-31d9-261a-a59d215629f4

appropriate at this time. RIPE Atlas data is not about user populations and their behaviors per se, but it addresses other important matters and the method of data collection is quite different. For example, the network usage and the behavior that RIPE Atlas is through the lens of the probe operators that are more technical and savvy than the general population, so they can change their DNS resolvers. As Jim Cowie mentions, Atlas Probes's power users might not match to any meaningful consumer population. Atlas probe locations also are dense in areas such as Europe while not in other areas such as Africa and South Asia which can introduce significant bias for researchers. (See Jim Cowie's presentation) In the future, it might be possible to debias RIPE Atlas data to see what the data can reveal. This has been done before, for example, Fanou et al used RIPE data to understand how African ISPs used third party public resolvers.

Conclusions and recommendations

DNS resolvers' governance is evolving rapidly, and the centralization and the consolidation of services are in need of monitoring. While centralization may yield benefits like enhanced security and efficiency, it also raises concerns about market dominance and accessibility. This report highlights the diverse motivations and challenges faced by ISPs and network operators in adopting or providing DNS resolvers, shaped by factors such as regulatory pressure, operational costs, and technological capabilities.

Our findings reveal a global decline in the use of public DNS resolvers, with regional variations influenced by local conditions, political events, and economic constraints. The correlation between DNS resolver adoption and factors like Internet freedom, GDP, and press freedom demonstrates the complexity of this ecosystem, demanding nuanced analysis that moves beyond geographic boundaries to consider the unique characteristics of network operators.

As we move forward, it is imperative to address barriers to market entry for new DNS resolver providers, promote decentralization where feasible, and mitigate the risks of over-regulation. Supporting open-source initiatives and fostering collaboration among stakeholders can ensure a resilient and inclusive DNS infrastructure that meets the needs of diverse user communities worldwide.

This research underscores the need for continued monitoring and innovation to lead to redistribution and re-decentralization of DNS resolvers through making the provision of resolvers easy and sustainable.

Centralization is as a result of consolidation of tech services in the hands of a few companies. While it is not inherently a bad thing and centralization could actually be useful in bringing more security, the trend needs to be monitored for market barriers. In our research, we tried to understand why there are so few public DNS resolvers in the market and tried to uncover some of the answers by asking network operators and ISPs in specific what their incentives and deterrents were in using public DNS resolvers instead of their own.

It is important to note that using public DNS resolvers can be beneficial especially for Internet freedom and security. Different vulnerable communities have used public DNS resolvers to circumvent censorship or have a more secure connection during political events.

Andrew Sullivan (the then CEO of the Internet Society) highlighted that it is an actual debate whether it is healthier for the Internet for ISPs to provide their own resolvers, or to rely on third-party resolvers. There is one argument that ISPs should provide their own resolvers, which can be better for local performance, and allow for some control over content and security. There is another argument that it is better to rely on third party public DNS resolvers because ISPs may not have the resources and capacity to provide adequate DNS resolvers and that such services are best provided by those who are focused on them.

So our aim should be twofold: monitor market barriers and prevent further centralization in the DNS market, help with decentralization of the DNS resolvers operator through taking the following actions :

- Monitor the potential centralization of public DNS resolvers and help network operators to choose the best course of action when it comes to deciding whether to outsource or provide their own resolver
- Enable as many DNS resolvers to enter the market as possible
- Reduce regulatory overreach that could hamper access to a globally connected DNS
- Provide open source infrastructure and best practices

Recommendations

1. **Promote Decentralization and Diversification:**
   - Encourage the entry of more DNS resolver providers to reduce reliance on a few dominant players.
   - Support open-source initiatives and collaborations to create accessible and scalable DNS solutions.
2. **Reduce Regulatory Overreach:**
   - Advocate for balanced regulations that do not impose excessive burdens on DNS resolver operators, particularly non-profit and smaller providers.
   - Work with policymakers to ensure that regulations like content filtering and blocking orders are transparent, proportionate, and do not hinder global DNS connectivity.
3. **Enhance Data Sources for Monitoring Trends:**
   - Diversify data sources beyond APNIC to gain a more comprehensive understanding of DNS resolver usage.
   - Explore debiasing methods for existing datasets, such as RIPE Atlas data, to minimize regional or socio-economic biases.
4. **Shift Analytical Focus:**
   - Move away from purely regional or country-level analyses and instead focus on network operator characteristics, such as size, business type, and operational needs, to better understand trends in DNS resolver adoption.
5. **Support Smaller ISPs and Vulnerable Communities:**
   - Provide resources, training, and incentives to smaller ISPs to develop and maintain their own DNS resolvers.
   - Highlight the role of public DNS resolvers in supporting vulnerable communities during political events or times of unrest.
6. **Monitor Centralization Risks:**
   - Develop tools and methods to track market consolidation and identify potential barriers to competition in the DNS resolver ecosystem.
   - Collaborate with organizations like the Internet Society and technical standards bodies to advocate for policies that preserve Internet openness.
7. **Leverage Partnerships and Collaborations:**
   - Foster partnerships between DNS providers and other stakeholders, such as ISPs, IXPs, and browsers, to improve the performance and reach of DNS services.
8. **Educate End Users and Network Operators:**

- Raise awareness about the benefits and trade-offs of using public versus local DNS resolvers.
- Provide clear and accessible guidance on best practices for DNS resolver deployment and management.

How to use our research and data analysis:

As we mentioned throughout this report, we used APNIC's data on DNS resolvers to understand the use of public DNS resolvers. We put all the data and what we have done so far in GitHub under DNStories. You can access it here: https://github.com/DNStories/DNStories

Meetings, publications and others:
A range of publications, presentations and meetings about this issue has been listed here: https://digitalmedusa.org/projects/resolved-dns/

Overview of the DNStories Repository

The DNStories repository contains various files related to DNS analysis, including datasets, Python scripts, Jupyter notebooks, and documentation. These resources are intended to assist in understanding and visualizing DNS resolver usage across different regions. We have the data from June 2022 to June 2024.

Repository Structure

- **Datasets (`.csv` and `.xlsx` files):** These files contain data on DNS resolver usage, such as `australia-open-resolver-usage.csv` and `apnic-monthly-data.xlsx`.

- **Python Scripts (`.py` files):** Scripts like `download-apnic-data.py` and `local_utils.py` are used for data processing and analysis.

- **Jupyter Notebooks (`.ipynb` files):** Notebooks such as `Create CC m49 map.ipynb` and `Visualize changes.ipynb` provide interactive data analysis and visualization.

- **Documentation (`.md` files):** Files like `README.md` and `CODE.md` offer explanations and guidelines for using the repository's resources.

How to Use the Repository

Clone the Repository: To work with the repository locally, clone it using Git:

bash
CopyEdit

```
git clone https://github.com/DNStories/DNStories.git
```

2. **Explore the Data:** Review the datasets available in `.csv` and `.xlsx` formats to understand the scope of data provided.

3. **Utilize Python Scripts:** Use scripts like `download-apnic-data.py` to fetch additional data or `local_utils.py` for data processing tasks.

4. **Interact with Jupyter Notebooks:** Open notebooks such as `Create CC m49 map.ipynb` in Jupyter to visualize and analyze data interactively.

5. **Refer to Documentation:** Consult `README.md` and `CODE.md` for detailed instructions and explanations on using the repository's resources effectively.

About .IE

.IE is the national registry for Ireland's country-code top-level domain (ccTLD). As a key player in Ireland's internet infrastructure, .IE is responsible for maintaining the .ie namespace and ensuring its security, stability, and resilience. The organization plays an active role in promoting digital trust, supporting research, and engaging with stakeholders to strengthen Ireland's digital ecosystem. Through initiatives focused on cybersecurity, internet governance, and infrastructure transparency, .IE contributes to the broader conversation around internet resilience and sovereignty in Europe.
weare.ie

About Digital Medusa

Digital Medusa is a nonprofit organization focused on safeguarding internet infrastructure, defending digital rights, and promoting transparency in the governance of the internet. Through research, advocacy, and capacity building, Digital Medusa works with technical communities, civil society, and policymakers to examine emerging threats to the open internet. Its work on DNS resolvers, censorship, and digital trade is part of a broader mission to ensure that the internet remains a free, secure, and interoperable public resource.
digitalmedusa.org

About Digital Internet Infrastructure Fund:

The D//F (Digital Infrastructure Insights Fund) is a multi-funder initiative by Ford Foundation, Alfred P. Sloan Foundation, Omidyar Network, Schmidt Futures and Open Collective sustaining a platform for researchers and practitioners to better understand how open digital Infrastructure is built and deployed.
https://infrastructureinsights.fund/

Appendix 1

Glossary of Terms

Anycast DNS:
A network addressing and routing method that allows multiple servers in different locations to share the same IP address. Traffic is routed to the

nearest server, improving speed and reliability.

Autonomous System Number (ASN):
A unique identifier assigned to networks on the Internet that enables them to exchange routing information.

Caching:
The process of storing data temporarily to reduce retrieval time. In DNS, caching helps reduce latency by storing resolved domain names locally.

Centralization:
The concentration of Internet services or infrastructure in the hands of a few entities, potentially leading to reduced diversity and resilience.

Content Delivery Network (CDN):
A geographically distributed network of servers that delivers web content efficiently by caching data closer to users.

DNS Blocking:
A censorship method where access to specific domains is restricted by preventing their resolution to IP addresses.

DNS Resolver:
A server or software that translates domain names (e.g., example.com) into IP addresses required for Internet connectivity.

DNS-over-HTTPS (DoH):
A protocol for performing DNS resolution over encrypted HTTPS connections, enhancing privacy and security.

Digital Sovereignty:
The concept of a nation's ability to control its own digital infrastructure and data within its jurisdiction.

Domain Name System (DNS):
A hierarchical system that maps human-readable domain names (e.g., www.google.com) to machine-readable IP addresses.

Extraterritorial Laws:
Regulations enforced by a country on entities or individuals located outside its borders, often affecting global DNS operators.

Freedom House Internet Freedom Index:
A measure assessing Internet freedom in countries, considering factors

like censorship, surveillance, and access restrictions.

IETF (Internet Engineering Task Force):
An open standards organization responsible for developing and promoting Internet protocols, including DNS standards.

Internet Exchange Point (IXP):
A physical infrastructure allowing different networks to interconnect directly, reducing latency and improving speed.

Latency:
The delay between a user's action and the server's response. In DNS, latency affects how quickly a domain name resolves.

Net Neutrality:
The principle that Internet service providers should treat all data equally, without discrimination or favoring certain services.

Open Resolver:
A DNS resolver accessible by anyone on the Internet, not restricted to a specific network.

Public DNS Resolver:
A DNS resolver service open to the public, often provided by companies like Google (8.8.8.8) or Cloudflare (1.1.1.1).

Recursive DNS Resolver:
A type of DNS server that queries multiple other servers to resolve a domain name and return the result to the user.

Regulatory Landscape:
The framework of laws and policies governing DNS resolver operations and Internet services.

Resolver Adoption:
The process by which ISPs or users opt to use specific DNS resolvers, either public or local.

Transaction Cost Economics:
An economic theory that explains organizational decisions, such as outsourcing or providing DNS resolvers, based on costs related to search, bargaining, governance, and uncertainty.

Transparency Report:

A document released by organizations detailing how they handle user data, comply with regulations, or address government requests, such as blocking orders.

Unicast DNS:
A traditional DNS setup where one IP address corresponds to a single server, potentially leading to inefficiencies during outages or heavy traffic.

Zone File:
A file containing mappings between domain names and IP addresses, stored on authoritative DNS servers.

Appendix 2

Jim Cowie’s method on RIPE ATLAS

I downloaded and pooled all measurements from two long-standing RIPE Atlas measurements from April 2017 through July 2024, of which about 2.6 billion measurements returned an IPv4 result from one of:

- https://atlas.ripe.net/api/v2/measurements/8310245
    - ("dig -t A whoami.akamai.net")
- https://atlas.ripe.net/api/v2/measurements/8310237
    - ("dig -t TXT o-o.myaddr.l.google.com")

Both of these return the address of the recursive resolver that is seen at the authoritative server; that is, if you are using Google public DNS, the second one might return

```
;; ANSWER SECTION:
o-o.myaddr.l.google.com. 60    IN     TXT   "edns0-client-subnet 64.35.200.0/24"
o-o.myaddr.l.google.com. 60    IN     TXT   "172.253.195.210"
```

...which would show that you connected to an instance of 8.8.8.8 that eventually ended up passing your question through one of the Google recursive servers in 172.253.195.192/26, which happens to be in their Virginia datacenter.

I reduced these to monthly statistics by counting successful IPv4 queries in each of five categories, according to the recursive resolver address returned:

- [SameASN] ... resolver in the same ASN that hosts the atlas probe
- [Google] ... resolver in AS15169 (google)
- [Quad9] ... resolver in AS19281 (Quad9) or by AS42 (PCH/Woodynet)
- [Cloudflare] ... resolver in AS13335 (Cloudflare)
- [Other] ... none of the above

The attached dataset is indexed by month, and by probe country code, or by probe region.

Fields are:

- created: month in which measurement was performed
- country: two-letter country code
- region: world region for country code
- probe_count: total number of participating probes
- total: count of measurements performed
- same_asn: count of measurements classified as [SameASN]
- google: count of measurements classified as [Google]
- quad9: count of measurements classified as [Quad9]
- cloudflare: count of measurements classified as [Cloudflare]
- other: count of measurements not otherwise classified
- same_asn_pct: percentage of measurements classified as [SameASN]
- google_pct: percentage of measurements classified as [Google]
- quad9_pct: percentage of measurements classified as [Quad9]
- cloudflare_pct: percentage of measurements classified as [Cloudflare]
- other_pct: percentage of measurements not otherwise classified

Since the number of probes and the number of measurements per probe can vary (and the first and last months are not complete), it's probably best to just use the percentages to determine the trends.

Two files are attached:

- recursive_summary.csv.gz ::: sums and percentages by country
- regional_resolvers.csv.gz ::: sums and percentages by world region

The regional memberships are arbitrary, and I could redo them if you have a scheme you like better, but it should give a sense for regional trends:

```
regions = {
    'Australia and New Zealand': 'AU CX CC HM NZ NF',
    'Central Asia': 'KZ KG TJ TM UZ',
    'Eastern Asia': 'CN HK JP KP KR MO MN TW',
    'Eastern Europe': 'BY BG CZ HU MD PL RO RU SK UA',
    'Latin America and the Caribbean': 'AI AG AR AW BS BB BZ BO BQ BV BR
KY CL CO CR CU CW DM DO EC SV FK GF GD GP GT GY HT HN JM MQ MX
MS NI PA PY PE PR BL KN LC MF VC SX GS SR TT TC UY VE VG VI'
,
    'Melanesia': 'FJ NC PG SB VU',
    'Micronesia': 'GU KI MH FM NR MP PW UM',
    'Northern Africa': 'DZ EG LY MA SD TN EH',
    'Northern America': 'BM CA GL PM US',
    'Northern Europe': 'AX DK EE FO FI GG IS IE IM JE LV LT NO SJ SE GB',
    'Polynesia': 'AS CK PF NU PN WS TK TO TV WF',
    'South-eastern Asia': 'BN KH ID LA MY MM PH SG TH TL VN',
    'Southern Asia': 'AF BD BT IN IR MV NP PK LK',
    'Southern Europe': 'AL AD BA HR GI GR VA IT MT ME MK PT SM RS SI ES',
    'Sub-Saharan Africa': 'AO BJ BW IO BF BI CV CM CF TD KM CG CD CI DJ
GQ ER SZ ET TF GA GM GH GN GW KE LS LR MG MW ML MR MU YT MZ NE
NG RE RW SH ST SN SC SL SO ZA SS TZ TG UG ZM ZW',
    'Western Asia': 'AM AZ BH CY GE IQ IL JO KW LB OM PS QA SA SY TR AE
YE',
    'Western Europe': 'AT BE FR DE LI LU MC NL CH',
}
```