Technological Background and Public Position on Behalf of the Israeli Internet Association (ISOC-IL)

Proceeding 33367-05-2023 ZIRA v. Google

Table of Contents

Authors:
Dr. Assaf Wiener, VP of Research and Public Policy, Israeli Internet Association (ISOC-IL)
Attorney Yoram HaCohen, CEO, Israeli Internet Association (ISOC-IL)

December 2025

A. About Israeli Internet Association (ISOC-IL): Expertise and Professional Experience for the Benefit of the Public Interest

The applicant, the Israeli Internet Association (ISOC-IL), is a registered association number 580299543, which began operating in 1994 and was registered as an association in 1997, as a non-governmental, independent and non-profit body, which manages, for the benefit of the Israeli public, essential Internet infrastructures that are at the core of Internet activity in Israel. The applicant is managed by Attorney Yoram HaCohen (who also co-wrote this document), who reports to a seven-member board of directors who work on a voluntary basis and employs approximately 30 employees, most of whom are experts in technological, legal and public policy issues related to the Internet.[1]

The applicant is acting as a professional and non-profit body operating for the benefit of the general public in Israel. Among its other activities, and the main one, the applicant manages the national top-level domain name registries (Domain Names Registry) of Israel (ccTLD – Country Code Top Level Domain) with the extensions: ".il" and ".Israel"; as well as the Israeli Internet Exchange (IIX – Israeli Internet Exchange). The applicant is defined by the state, since 2018, as an operator of a "vital computer system" (critical state information infrastructure) as defined in the Security Regulation in Public Bodies Law, 5758-1998, and is therefore listed in the Fifth Schedule to the Law. This statutory status therefore expresses the importance of the technological activity with which the applicant is entrusted.

The applicant therefore has extensive expertise in the field of the Internet in general, and possesses unique and long-standing knowledge of how the DNS infrastructure and domain names operate in Israel.[2] The applicant is also a permanent member of the international civil society organizations that operate the Internet domain name infrastructures, which are at the core of the proceedings under consideration in court.

In this regard, the applicant is an active member, since its establishment, of the umbrella organization of European national domain name infrastructure operators: Council of European National Top-Level Domain Registries (CENTR), whose members possess extensive professional experience in various aspects of Internet infrastructure governance, and particularly in contemporary issues of blocking Internet sites used for illegal activity.[3] The applicant is also active within ICANN (Internet Corporation for Assigned Names and Numbers), the global organization that manages the operational infrastructure of the Internet, including the DNS Root Servers, through cooperation and coordination between governmental bodies, civil society, and industry. Additionally, the applicant serves as the Israeli chapter of the Internet Society (ISOC – Internet Society) – a professional, international, non-governmental and non-profit organization established in the early 1990s that promotes cooperation and coordination in the development of Internet technologies and applications.[4] The applicant participates from time to time in meetings of the global Internet Governance Forum (IGF) and represents Israeli civil society there.[5] In addition, the applicant also serves as a LIR (Local Internet Registry) for many IP address spaces allocated to Israel, within the framework of the European Regional Internet Registry (RIR) RIPE-NCC.

Beyond operating the aforementioned essential infrastructure services, the applicant has proven experience and a long track record of promoting the public interest in various aspects of Internet law

---

[1] Association bylaws and detailed activity reports throughout the past decade are available at: https://www.isoc.org.il/about

[2] See for example: Israeli Internet Association, Summary of the Year 2024 in the .il and .Israel Domain Name Spaces [link].

[3] See: https://www.centr.org/about/about-centr.html

[4] See: https://www.internetsociety.org/about-internet-society

[5] See for example: https://en.isoc.org.il/about/news-room/isoc-il-euvp-igf-2025

and technology,[6] and serves as a reliable and neutral source of knowledge for the legislative branch[7] and the judiciary.[8]

Therefore, given the applicant's proven expertise and experience in the issues arising in the current proceeding and due to the broad implications of this matter, as will be described below – implications that extend beyond the framework of the specific dispute – the applicant wishes to present this survey to the Honorable Court hearing the proceeding, so that the full and balanced picture may be before it, and in order to present to it the comprehensive public interest, which extends beyond the economic interests of the direct parties to the dispute.

B. The Technological Infrastructure Required to Decide on the Proceeding

The technology community and the official Internet engineering institutions have, over the past decade, provided essential factual foundations for the legal discussion regarding the necessity, proportionality, and effectiveness of judicial orders for blocking or restricting access to illegal content at the infrastructure level. This is distinct from the discussion regarding the liability of hosting service operators or online platforms for illegal content.

As will be detailed below, the technological and normative basis for distinguishing between Internet access providers (ISPs) and Public DNS Resolvers and the manner of DNS operation requires, in the applicant's view, rejection of the expansive interpretation of the term "access provider" – an interpretation proposed by the plaintiffs and supported by the position of the Legal Advisor to the Government – for the application of access restriction orders provided in Section 53A of the Copyright Law.

B.1 The DNS System as Core Infrastructure of the Internet as a Global, Open, and Reliable System

The protocol that defined the domain name mechanism,[9] and the Domain Name System (DNS – Domain Name System) operating under it, are an integral and significant part of the day-to-day functioning of the Internet and its use. The DNS is responsible for the vital task of translating domain names, which are textual descriptions comprehensible to humans for computing/communications resources on the Internet, into IP addresses at which those resources operate. Computers require IP

---

[6] See for example: Israeli Internet Association, IPv6 Deployment in Israel: A Policy Document (2018); Israeli Internet Association, The Internet of Things (IoT) in Israel: Benefits, Challenges and Policy Recommendations (2022); Israeli Internet Association, Not Holding the Line – The Social Networks' Response to Offensive and Terror-Supporting Content in the October 7 Attack and Operation Swords of Iron (2024).

[7] Recent examples of participation and submission of background materials to Knesset committee discussions: Science and Technology Committee on accessibility of digital services (22.1.2025); Special Committee on Children's Rights of the Knesset on the right to be forgotten (14.1.2025); Committee on Public Initiatives on communication with public bodies law (29.1.2025); Science and Technology Committee, on the use of artificial intelligence for image forgery and dissemination of false information in the Israel-Hamas war in Gaza (professional survey at the request of the Subcommittee on Artificial Intelligence and Advanced Technologies, 19.12.2023).

[8] See for example: HCJ 748/24 Avital v. Legal Advisor to the Government (12.11.2024), at para. 14, as an example of judicial reliance on the applicant's research outputs and ongoing data on the Israeli Internet.

[9] The protocol is formulated and published by the Internet Engineering Task Force (IETF), which is the professional body responsible for developing the technological standards for the operation of the Internet as a global and decentralized network. It was formulated starting in 1983 in two documents, RFC 882 and RFC 883 (https://datatracker.ietf.org/doc/html/rfc882, https://datatracker.ietf.org/doc/html/rfc883), which were updated over the years. Today the valid text is detailed in RFC 1035 (https://datatracker.ietf.org/doc/html/rfc1035).

address information to reach those resources that serve all devices and online services connected to the network (such as a web server hosting any website, an email server, a streaming distribution server, etc.). The DNS also has less visible infrastructure functions upon which day-to-day Internet use relies.[10]

The DNS system on the Internet was designed and implemented from its inception as a globally distributed and redundant system that does not allow a single commercial or governmental entity to control all the information and access channels to it. This is achieved through a multi-layered, hierarchical, redundant, and distributed structure.

Internet access providers (ISP – Internet Service Provider) provide the user with the physical medium between the end user and the core backbone of Internet communications. Data communications between the end user and Internet services take place over this physical medium. By virtue of this, ISPs are local in nature, as they enable digital services provided over the physical medium. Among these services, the end user is enabled access to the Domain Name System as an infrastructure service essential to the operation of every device connected to the Internet.

The Domain Name System is not based solely on Internet access providers, but on a global, independent, and decentralized system of servers linked to domain name registries – which in turn update the information required for DNS operation on an ongoing basis.

We will detail the main components of DNS operation:

- **Authoritative DNS Servers** – These are computer servers that respond to queries using the DNS protocol. Within this framework, authoritative DNS servers provide authoritative and accurate information about the next server that must be queried to complete the required information, or provide the final answer to the question: what is the IP address serving the Internet service the user wishes to access? For example, ICANN is responsible for the authoritative DNS servers at the top of the Internet hierarchy, called Root Servers, and makes them publicly accessible; the Israeli Internet Association manages and makes accessible the authoritative DNS server for IL; the National Digital Agency manages and makes accessible the authoritative DNS server for gov.il; and the Courts Administration manages and makes accessible the authoritative DNS server for court.gov.il.
- **Recursive DNS Servers (Resolvers)** – These DNS servers query, at the request of an end user, authoritative DNS servers using the DNS protocol and at the end of the process convey to the end user the IP address of the Internet service that the user wishes to reach and use.

To illustrate, using a common though imprecise metaphor, the authoritative servers are a kind of entries in giant "phone books"[11] containing information about the "phone numbers" – or, IP addresses – of domain names at which remote servers operate. The recursive server is a kind of "directory assistance operator," which itself does not hold any information about IP addresses, but when it receives a query with a particular domain name, it knows how to locate in the "phone books" entries the IP address associated with the requested domain name. After locating the IP address, the recursive server conveys it to the end user who initiated the query, and thus the user can contact the requested server. It should be emphasized: the recursive server does not itself hold IP addresses and also does not participate in creating the physical connection between the end user and the remote server. It merely locates the information needed to create the connection, and nothing more. On the other side, the authoritative server can change, in an instant, the IP address associated with a domain name upon

[10] Such as managing virtual servers and microservices, internal organizational networks, resource balancing, smartphone applications, information security and cyber defense, the Internet of Things (IoT), etc.

[11] The metaphors below are provided for simplification and illustration purposes only and should not be considered binding (see, e.g., the article by Dr. Abraham N. Tennenbaum, On Metaphors in Computer and Internet Law, Sha'arei Mishpat 4(2), 2006 (link)).

instruction from whoever manages it. This means that if the IP address is known to the user from another source, there is no need for a recursive server at all, and the user can connect to the remote server directly, using the critical infrastructures for creating the connection – among them, the Internet access provider (ISP), which, as stated, provides physical access to the Internet.

- Most ISPs (Internet access providers) operate Resolvers (that is, recursive resolution services) as a component of the connectivity services they provide to end customers. Also operating such Resolvers are providers of "free" DNS services, such as the one operated by Google that is at the heart of this proceeding. It is important to note that operating DNS Resolvers is not the exclusive domain of Internet access providers and "free" DNS service providers. Resolvers are also regularly and independently installed in businesses, large and small, that manage internal computing networks,[12] and can even be installed by end users.

As stated, Internet access providers, as part of the bundle of services they provide to their customers, also provide recursive DNS services (resolvers). In Israel, operating a Resolver by an ISP is not required by license, nor is it a condition under the Communications (Bezeq and Broadcasting) Regulations (General Permit for the Provision of Communications Services), 5783-2022, so this is a voluntary activity by the providers as a service to their customers. In fact, ISP services can be provided without providing resolving services. Historically and operationally, on end user devices such as personal computers, tablets, or smartphones, the default setting is that the device contacts the Resolver operated by the Internet access provider through which the device is connected to the network.

Thus, the end user can, by changing settings (at the software, operating system, or physical network equipment level), configure other resolvers to perform DNS queries. That is, as long as end users do not change the default settings in their device operating systems or in the modems/routers connecting the local network to the Internet, the DNS Resolving process for computers and devices connected to the network is performed through the Internet access provider (ISP), to which the users' DNS queries are directed.[13]

- **Domain name registries** – These are services that manage central databases of the Top Level Domain (TLD) for which they are responsible (for example, the Israeli Internet Association manages the database of Israel's TLD, IL). This database records the details of domain names registered in the top-level domain. The registry, among other things, verifies that a particular domain name is not assigned twice; records the names of the authoritative DNS servers (name servers) serving the same domain name; and distributes this information to the DNS. The information is distributed by the registry to the authoritative DNS servers it manages, and is available for query by Resolvers. Unlike traditional registries, such as the Population Registry or the Land Registry, all information about the IP addresses of all domain names on the Internet is not found in a single database, but is organized and managed in a distributed and hierarchical manner.

Diagram 1: Overview of the entities taking part in the DNS system[14]

We will explain how DNS works with an everyday example of Internet use:

---

[12] For example, the Israeli Internet Association as a non-profit organization with a variety of activities and processes operates such a server on its internal network; it does not use the resolver of the ISP to which it is connected, nor a free DNS server such as the respondent. Government ministries also use an internal resolver on the network they manage, as do large corporations such as IBM, Intel, Microsoft, Google, etc.

[13] It is important to emphasize that the use of the ISP as the default for DNS query referral is characteristic of private users and small businesses, while large organizations typically direct their DNS queries to cloud services (such as AWS, Azure, or Google) or operate their own DNS Resolvers.

[14] OECD, Security of the Domain Name System (DNS) – An Introduction for Policy Makers, 12 (2022). Attached as Annex 3.

- The DNS system is a system that holds information in a hierarchical manner, and it directs the requester to locate information in it from a higher level to a lower level. The starting point is the highest level, which is called the root level (root servers). Below it is the level of Top Level Domains (TLDs) such as .IL or .COM, etc.
- Let's say a user wants to access the "Net HaMishpat" system, which operates at the address: https://www.court.gov.il/ngcs.web.site/homepage.aspx. To access the system, the user's browser must know the IP address of the service called www, which operates under the domain name court, in the subdomain gov, which is located in the top-level domain il, which is one of the TLDs on the Internet. The process is as follows:
- The Resolver configured for the user contacts one of the copies of the 13 authoritative DNS root servers of the ICANN organization scattered around the globe and asks what the IP address of www.court.gov.il is. Since the root servers do not hold IP addresses of domain names, they refer the Resolver to the level below them – in this case, the authoritative DNS servers serving the IL top-level namespace.
- Similarly, IL's authoritative DNS servers do not hold the specific IP address of www.court.gov.il, and therefore they redirect the Resolver to the level below, which is gov.il.
- Even the authoritative servers that publish gov.il do not know the IP address of www.court.gov.il, and therefore redirect to the authoritative DNS server of the Courts Administration, which is responsible for the domain names under court.gov.il.
- Now the Resolver asks the authoritative DNS server of court.gov.il what the IP address of the domain name www.court.gov.il is, and only it is "authorized" to give the required answer. As of this writing, the answer is the IP address 84.110.173.72. This information is sent from the Resolver to the user's computer, which can then use it to contact the requested resource (in this case, the web server called www.court.gov.il) and ask it to send the page called /ngcs.web.site/homepage.aspx (which is the home page of the "Net HaMishpat" system).

That is, although humans are used to reading and writing the domain name from left to right (i.e. www, then court, then gov, then il), the computer and the DNS look from right to left (first il, then gov, then court, and finally www).[15] Also, in locating information about a domain name with the .com extension (e.g. themarker.com), in addition to the root servers, completely different servers are involved that will answer the queries and provide the information required to reach the service.

B.2 The Technological and Public Value of Public DNS Resolvers as a Service Independent of Internet Access Providers (ISPs): Security, Privacy, and Decentralization

In recent years, a global trend has been established to move to the use of public DNS Resolving services, as commercial or free services available to any Internet user. This is a global, technologically advanced, and more secure alternative to traditional DNS services provided by Internet access providers as the default, which usually do not include a layer of security and encryption of DNS queries for the benefit of the user as is common in modern Internet traffic.[16] In addition, public DNS Resolving servers allow the user to choose protection services against malware or offensive content, according to their choice and the definition of the protection features by the service, and allow any

[15] The root servers are represented by a dot "." to the right of the top-level namespace (in this case IL), but it is customary to omit it.

[16] Based on extensions to the DNS protocol expressed in RFC 7858 defining DNS over Transport Layer Security (TLS) (https://datatracker.ietf.org/doc/html/rfc7858) and RFC 8484 defining DNS Queries over HTTPS (DoH) (https://datatracker.ietf.org/doc/html/rfc8484).

Internet user, from anywhere, to perform Resolving queries (while the DNS servers of Internet access providers allow service only to ISP subscribers).

Contrary to what is alleged in this proceeding, it is essential to clarify that global public DNS Resolving services are *not* "a portal to access infringing websites" and their nature is not to "facilitate the consumption of pirated content" or to "circumvent the law." This is a *legitimate* and highly valuable infrastructure in the architecture of the contemporary Internet as a global, distributed, and trusted system.

In fact, the technology community and Internet institutions have been emphasizing for many years the public value of public resolving services, such as those provided by the defendant and others as detailed below. Only recently did ICANN, the professional-technological body responsible for coordinating the various state and technological stakeholders in the operation of global Internet infrastructures, publish a working paper detailing the unique value of global infrastructure services of this type, in terms of stability, security, and protection of user rights:

"The landscape of DNS resolution has undergone a remarkable transformation in recent years, characterized by a significant rise in the popularity and utilization of public DNS resolvers. These resolvers, offered by various providers, have garnered widespread adoption due to their ability to deliver fast, reliable, and accurate DNS responses. Users are aware of the benefits of public DNS resolvers and have been reconfiguring their systems to leverage these services. This shift has been fueled by a growing understanding of the potential privacy and performance advantages that public resolvers offer over default DNS configurations, and in response to cases of state censorship and the abuse of DNS services offered by ISPs".[17]

In light of the increasing role of browser manufacturers and cloud service providers in developing encryption and security layers for Internet information traffic, these organizations are currently the prominent promoters of changes to the traditional model of the DNS system. This is done through the development and operation of DNS Resolving services and advanced protocols for securing and authenticating users' DNS queries. The most prominent of these are:

- Google Public DNS (8.8.8.8) – available to the public at address 8.8.8.8 since 2009.
- Cloudflare (1.1.1.1) – available to the public since 2018 at address 1.1.1.1.
- Quad9 (9.9.9.9) – a non-profit service available to the public since 2016 at address 9.9.9.9.[18]

Additionally, there are other services such as Apple Private Relay and governmental-state Public DNS Resolver servers such as DNS4EU in the European Union,[19] PDNS in England,[20] CISA in the United States,[21] and CIRA free public DNS resolver in Canada.[22]

The widespread adoption of these services by private users and organizations stems from the technological superiority they offer over the traditional Resolving process of Internet access providers, for example in operating mechanisms, at the user's choice, for preventing cyber attacks, or for

[17] ICANN Security and Stability Advisory Committee, DNS Blocking Revisited (2025), attached as Annex 2, in Section 6.1.

[18] Given the public value of public DNS Resolving services that protect privacy for Internet users, the Israeli Internet Association has hosted since 2019 at the Israeli Internet Exchange a local copy of the Quad9 service, which is operated by two non-profit organizations and IBM, and which improves the speed, efficiency, and security of Internet connectivity for users. See: https://www.isoc.org.il/news/online-url-repository-to-quickly-securely-and-privately-browse

[19] https://www.joindns4.eu/about

[20] https://nominet.uk/dns-services

[21] https://www.cisa.gov/resources-tools/services/protective-domain-name-system-dns-resolver

[22] https://www.cira.ca/en/canadian-shield/

implementing advanced DNS protocols that preserve privacy (DoH and DoT) or authenticate data (DNSSEC).[23]

In the current proceeding, the implication is that the characterization of public DNS Resolving services as a "portal to access infringing websites" or a "service for circumventing the law" as presented by the plaintiff should not be accepted. Similarly, the Legal Advisor to the Government's position that "public DNS services facilitate the consumption of pirated content" presents the nature of these services and their central purpose in the operation of the Internet as a global network enabling communication between networks (or Internet access providers) in a false light.

B.3 The Importance of Distinguishing Between a Recursive DNS Service (Resolver) and an Internet Access Provider (ISP)

As noted, Internet engineering is based on the technological and normative distinction between "Internet access providers" (ISPs) and "hosting" services on the one hand, and the various types of services in the global DNS infrastructure on the other. Therefore, although Resolvers are an important auxiliary tool for locating the information needed to access resources operating under domain names, it cannot be said that they must be provided by an external provider, and certainly their nature is not identical to the role of Internet access providers.

As a matter of fact, end devices with access to the Internet network are not required to rely on external Resolver services from the Internet access provider or a Public DNS Resolver such as the defendant, as end users also have the option of running their own private DNS Resolver on their home network that performs the queries and IP lookups by domain name with ease, on any operating system, using several freely available open-source software programs.[24]

The function of a DNS Resolver service, such as the one operated by the defendant, is *purely informational*: answering the question "what is the IP address of a particular domain name?" If the user knows the IP address, there is no need whatsoever for this service in order to access the desired domain directly. Furthermore, *the service is not involved at all in transmitting the website content or the actual data to the end user*. Its operation consists of automatically collecting information from authoritative servers and making it accessible to the user. In this respect, it is fundamentally different from an Internet access provider (ISP), which constitutes the physical and logical infrastructure for transmitting data, and from a technological perspective, it is incorrect to consider it an "access provider."

Applying the definition of "access provider" to such an informational service would, in the applicant's view, lead to *far-reaching and absurd results*. For example, today most access to websites on the Internet is not done by manually typing the domain name, but by entering appropriate search terms into one of the many public search engines (Google, Bing, Yahoo, and many others), which present the relevant website in the results, and thereby the user locates the desired domain name. This is an activity very similar to the operation of a DNS Resolver, at a different level (the search engine locates the domain name using search terms, and the DNS Resolver locates the IP address using the domain name). Under the proposed expansive definition, search engines would also constitute "access providers." Another example: access to websites today is in practice done almost exclusively through browsers (Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, and many others). Browsers constitute the platform for those search engines, enabling the location of domain names

[23] ICANN Security and Stability Advisory Committee, DNS Blocking Revisited (2025), attached as Annex 2, in Section 6.5.

[24] See for example: www.knot-resolver.cz; nlnetlabs.nl/projects/unbound/about; github.com/trickest/resolvers

using search terms. Should they too be considered "access providers" under Section 53A of the Copyright Law? Obviously not.

The absurdity is further sharpened in light of what was explained above, that many commercial and public entities – including government ministries – operate their own DNS Resolvers. Would it be correct to define the State of Israel or Intel or IBM as "access providers"? Would a private individual who installed an open-source DNS Resolver at their business or family home be subject to orders to block websites infringing copyrights as an "access provider"?

In the applicant's view, the examples above clarify the self-evident, which is that an "access provider" – as its name implies – is one who provides access to the Internet, and without whom *access* to the Internet is not possible at all. ISPs precisely meet this definition, since without the service they provide in connecting through the physical medium, it is impossible to connect to the Internet at all. By contrast, search engines, browser operators, and DNS server operators, public and private, provide services that greatly streamline browsing the web, but their use is not essential and they are not involved in creating the actual access between the end user and the remote server, and therefore they cannot fall within the definition of "access provider."

Like any Internet service, the Domain Name System uses Internet access providers around the world for connectivity to the Internet backbone and for making authoritative DNS servers accessible, but the DNS is, as stated, a global, independent, and decentralized system for managing domain name servers (fed from domain name registries with the various extensions on the Internet) and providing the information needed to link domain names and the IP addresses serving them.

The technological and substantive differences between Internet access providers (ISPs), which exclusively serve local end customers, and public DNS Resolving services, which are available as global infrastructure for any device connected to the Internet, therefore require rejection of the expansive interpretation of blocking order authority as proposed by the plaintiffs and the position of the Legal Advisor to the Government.

Even assuming that the legislative intent and the language of the legislation in Section 53A does not seek to limit the scope of authority only against Internet access providers (as basically defined in Section 4T(a) of the Communications Law as a service subject to licensing or dedicated regulatory supervision in Israel), there is still no justification for the interpretive expansion sought in this proceeding. In the absence of normative or technological justification bridging these gaps, the applicant believes that there is no basis for the interpretive expansion of the term "access provider" to also include DNS Resolving services operating in the core of the global Internet, given the essential difference between them and local ISP services.

In this regard, we wish to note that in 2022, Amendment No. 76 to the Communications (Bezeq and Broadcasting) Law, 5742-1982 was adopted by the Knesset, which significantly changed the regulatory framework for Internet services in Israel and significantly reduced the obligation to obtain a license for providing Internet access services, replacing it with registration in a dedicated registry. Despite this relaxation, services of the type managed by the defendant were not included within the new regulatory framework.

B.4 The Question of Territoriality and Applicability of Blocking Only to Users from Israel

The plaintiffs' unprecedented request for an access restriction order against Public DNS Resolvers at the core of the global Internet – as distinct from the existing law and practice in Israel for issuing such orders against Internet access providers (which contract directly with customers in Israel) – raises legal questions regarding the territorial applicability of Section 53A and the authority of Israeli courts to compel *global* services to corrupt their DNS responses for users from Israel *only*.

Alongside the legal discussion on this point, it is important to emphasize that the position seeking to apply orders to global DNS providers rests on a disputed technological assumption that these entities can easily perform precise territorial blocking. The Legal Advisor to the Government's position, and the expansive interpretation she proposes for the term "Internet access provider" in the circumstances of this matter, is based on the caveat that "there is reason for the requested order – insofar as it is decided to issue one – to be territorially circumscribed so that its legal applicability is in Israel only."[25] However, there is no factual basis for the assumption underlying the aforementioned legal balance, according to which providers of global DNS Resolver services are able to reliably and efficiently distinguish between the geographic location of devices using the service and apply selective blocking if (and only if) the users are within the jurisdiction of Israel. This is because the DNS protocol is designed to be "blind" to the geographic location of the user, and the operation of global root servers is not built to filter queries based on the country of origin.

At the technological level, the various DNS protocols do not support filtering queries based on any geographic origin whatsoever. They do not take part in the protocol and root server system of the Internet's domain name architecture, where user identification is performed after establishing a connection with the server. Accordingly, a public resolver intended to serve any device connected to the Internet is not built and not designed to distinguish, or discriminate, between those who contact it. On the other hand, it is supposed to be able to verify that its services are not being abused, since cyber attacks can be carried out using free resolving services. Therefore, the resolver's primary resources will be devoted to preventing abuse of its services, and not to providing different answers to queries based on the geographic origin of the service request.

In our case, this means that the expansive interpretation extending the circle of liability under Section 53A to DNS Resolvers through judicial legislation, as requested in this proceeding, cannot be accepted without an in-depth factual examination of the means and reliability of geographic filtering of queries in the public resolver, in order to ensure the necessary proportionality against the concern of harm to Internet function and/or users as a result of error (positive or negative) in geographic identification. In order for a server to filter queries based on geographic origin and decide whether the requester is Israeli (and then withhold the information about the infringing site and display the message determined by the court) or is not Israeli (and then provide the information about the site), it must connect to external information services for inferring the geographic location of an IP address at a particular point in time – which are not considered, or even claim to be, fully accurate and reliable. The geographic attribution of IP addresses is changing information, because due to the shortage of IPv4 IP addresses, there is active trading in these addresses, and addresses originating from one geographic area may be in use by an entity in another geographic area.

The technological-engineering and operational limitations of inferring geographic location based on IP addresses on the global Internet[26] have forced even the most advanced technological services on the market today to explicitly emphasize that the accuracy of the process cannot be guaranteed, particularly in countries outside the United States. For example, MaxMind, which operates the most extensive geographic databases in the field and provides IP Geolocation services to hundreds of thousands of organizations worldwide, including major technology companies and government agencies, itself states:

"It is not possible for us to guarantee 100% geolocation accuracy. Accuracy exhibits high variability according to country, distance, type of IP (cellular vs. broadband, IPv4 vs. IPv6), and practices of ISPs. We do not guarantee exact matches to our competitors' data, nor identical accuracy to theirs, as

[25] Paragraph 6 of the Legal Advisor to the Government's opinion.

[26] See for example: Yuval Shavitt and Noa Zilberman, A Geolocation Databases Study (IEEE, 2011).

we may use different data providers in some instances… Some IP addresses cannot be located with the same accuracy as others…"[27]

The fact that the geoip information on which the resolver is supposed to base its decision is not 100% accurate may lead to two types of error – a first-order error (the address is Israeli, but the information about it is incorrect and therefore the site will not be blocked), and a second-order error (the address is not Israeli, but the resolver identifies it as Israeli and blocks access).[28] By contrast, when blocking is done at the ISP level, there are no errors (or their rate is minimal), since the entity contacting the resolver is a customer (paying in the target country) of the local ISP.

In summary, in order to limit blocking to users located in Israel only, the DNS Resolver provider would have to collect information about the IP addresses of those contacting it with queries, and attempt to block only those addresses located in Israel, using external services. This means a significant infringement of the privacy of the DNS Resolver's users, and the imposition of significant costs on the service operator. Beyond the direct harm resulting from this both to users and providers, this would endanger the very model of public Resolving services, which on the one hand would lose the attractiveness of their high security profile, due to the need to now identify the addresses of those contacting the server, and on the other hand would also have high costs imposed on them that could make them economically unviable to operate. This is an undesirable situation, given the high positive value attributed to the existence of these public servers, as detailed extensively in the previous chapter. Therefore, a precedent-setting decision to expand the authority of Israeli blocking orders to also cover global infrastructure services, as requested in the current proceeding, cannot rely on interpreting the existing legal arrangement for this type of private enforcement remedy against ISP services operating in the state territory under a model of registered users.

C. Findings and Insights of Internet Institutions and the Technology Community on the Issue

Also in the current global arena, global Internet institutions and Internet engineering bodies in civil society, which represent technological expertise and the public interest, emphasize the vital importance of the *technological and normative distinction* between "Internet access providers" (ISPs) as an end-user service and the various types of service providers in the DNS infrastructure and beyond.[29]

The technology community warns that blurring the boundaries between these layers and imposing blocking orders on global DNS Resolving services constitutes a dangerous change in network architecture. Such a move turns neutral infrastructure, whose function is to serve all users equally, into a tool for enforcing local policy, creating technical inconsistencies and undermining trust in the core systems of the Internet.

The technology community emphasizes the importance of distinguishing between the different layers of Internet infrastructure and the different entities operating them, including the distinction between the liability regime of Internet access providers (ISPs) versus DNS Resolving services. This distinction

[27] https://support.maxmind.com/knowledge-base/articles/maxmind-geolocation-accuracy

[28] A recent example of the reliability limitations of geographic location identification of Internet networks in the Israeli context, which was conveyed to the Israeli Internet Association by the Ministry of Communications and local Internet providers in September 2025, concerns the erroneous automatic classification of major communications networks in Israel (HOT and Wecom) as belonging to the State of Palestine. The Israeli Internet Association is also aware of a wide range of IP addresses used by entities operating in the Palestinian Authority but technically attributed to the State of Israel due to the history of IP address allocation to the region in the 1990s.

[29] Internet Society, A Policy Framework for Internet Intermediaries and Content (2025) – attached as Annex 1.

serves as the basis for examining the differing degree of liability of each of the layers in dealing with illegal content transmitted through them and the widespread effects of disrupting their operation through judicial orders in private proceedings.

Accordingly, the technology community and Internet institutions in civil society have in recent years warned against expanding the liability of DNS-type Internet infrastructure for dealing with copyright infringements by users, as distinguished from hosting services or local Internet access providers. This is due to the technical limitations and risks associated with disrupting the global DNS system.

An in-depth technical analysis published by the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF) as early as 2016 details and emphasizes the undesirable consequences of blocking mechanisms – particularly when they are applied to global connectivity services such as the DNS system and IP-based protocols. This type of intervention, the technology community warns, may cause widespread collateral harm, even if unintended, resulting from disruption of core technical functions upon which the Internet network relies.[30]

Since then and throughout the past decade, the insights of the professional community and the dialogue between stakeholders on this global issue of network governance are evident in the professional reports of the Internet Society (hereinafter: ISOC), which is the leading professional institution in the global Internet community for professional and objective knowledge on Internet technologies and network architecture. The most recent ISOC reports warn explicitly and consistently against the unintended consequences of DNS blocking through judicial orders, including on the reliability, stability, and security of the national and global cyberspace:

"Domain blocking at the level of public DNS resolvers can have unintended consequences that extend beyond content control, directly affecting the online safety of users in countries where these services operate… This not only weakens the protective shield for individuals and businesses but may also reduce a country's overall cyber resilience by removing or impairing a trusted infrastructure layer."[31]

Based on the functional distinction between the different layers involved in Internet activity and identification of the technical limitations and unique risks of forcing blocking through state law on public DNS Resolvers, the current position of the professional community is clear and categorical:

"DNS lookup services should not be required to control illegal or unwanted content on the Internet. Blocking access to domain names through DNS lookup services (recursive DNS servers) creates significant risks of over-blocking content, preventing access, and fragmenting the Internet. Attempts to require content filtering via recursive DNS servers breaks the integrity of the DNS and will make it untrustworthy."[32]

In other words, public DNS services should not be required to serve as tools for monitoring or blocking content, as this *undermines the trustworthiness* of Internet infrastructure, harms national cyber resilience, and breaks the technical reliability and integrity of the Internet network. This is especially true given the *very limited effectiveness* of such blocking, which does not remove infringing content from the network, which remains accessible through simple technological tools available to any end user at the browser and operating system level.[33]

---

[30] Internet Architecture Board (IAB), RFC 7754 - Technical Considerations for Internet Service Blocking and Filtering (2016).

[31] Internet Society, Policy Brief: Perspectives on Internet Content Blocking (2025) – attached as Annex 7.

[32] Internet Society, A Policy Framework for Internet Intermediaries and Content (2025) – attached as Annex 1.

[33] Internet Society, Mandated DNS Blocking: Critical Considerations (2025) – attached as Annex 5, at p. 5. Security and Stability Advisory Committee (SSAC), DNS Blocking Revisited (2025), attached as Annex 2, in Section 4.

Similar findings and insights are also evident in the professional reports and position papers of ICANN, the professional-technological body responsible for coordinating the various state and technological stakeholders in the operation of Internet infrastructures and the operation of the DNS root servers. Like ISOC, this is a non-governmental body not owned by any commercial company, built on a unique model in which decisions are made by broad consensus of stakeholders, including representatives of states, technology companies, academia, civil society organizations, and private users.[34]

The clear professional position presented by ICANN against expanding blocking or forced disruption of public DNS services for the purposes of content monitoring or blocking is detailed in the report of the Special Committee on Internet Stability and Security at ICANN, published only recently, in May 2025.[35] In particular, the Internet architecture professionals at ICANN emphasize in this report the harm of state blocking orders, particularly in the context of copyright enforcement, to the reliability of Internet infrastructure and modern cyber defense services. A key example of this is the disruption of DNSSEC mechanisms, which is the protocol adopted in recent years to ensure the authenticity of DNS data through cryptographic means. According to the report, when a resolver modifies the DNS response to enforce blocking or redirection, this action breaks the cryptographic chain of trust of DNSSEC.[36]

These current insights from the technology community of Internet infrastructure are also evident in the grave report published by the Internet Infrastructure Coalition in 2025, which details the dangerous impact of state orders on infrastructure services at the DNS layer, based on several prominent test cases from recent years (attached, Annex 6).

In our case, the technology community's insights provide a severe and clear warning against the use of core Internet infrastructure as a means of dealing with unwanted content, and in particular the dangers and ineffectiveness of blocking orders against Public DNS Resolvers. These blunt tools harm the critical core infrastructure of the Internet – which includes Recursive Resolvers and encryption protocols designed to support large-scale operations, speed, and security, and not to serve as censorship tools. Therefore, when neutral infrastructure systems are forced to perform content blocking, the result is not precise enforcement, but the creation of systemic risk that includes over-blocking, service disruption, and fragmentation of the global Internet.[37]

D. Normative Meanings and Considerations for Interpreting the Scope of Application of Access Restriction Orders Under Section 53A of the Copyright Law and the Interpretation of the Term "Access Provider"

The technological and normative differences between "*Internet access providers (ISPs)*" that exclusively serve local end customers, and public DNS Resolving services that are available *as global infrastructure for any device connected to the Internet*, as detailed in the previous chapter, require, in the applicant's view, rejection of the expansive interpretation of blocking order authority as proposed by the plaintiffs and the position of the Legal Advisor to the Government.

---

[34] For further discussion of the role and status of ICANN in Internet governance, including the operation of the DNS root servers of the global system, see above in Part A.

[35] ICANN Security and Stability Advisory Committee (SSAC), DNS Blocking Revisited (2025), attached as Annex 2, in Section 6.5.

[36] In this context, the meaning of "DNS blocking" is that the resolver will intentionally provide an incorrect answer to users' queries regarding a defined domain. That is, instead of directing to the IP address of the requested domain name, it provides information directing the requester to a different address, in order to view the message determined in the access restriction order.

[37] Internet Infrastructure Coalition, DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet (2025), attached as Annex 6.

In addition, there are also weighty legal-normative reasons for rejecting the expansive interpretation proposed by the plaintiffs and the Legal Advisor to the Government's position regarding the term "access providers" in Section 53A of the Copyright Law, as detailed below.

D.1 The Public Interest and the Principle of the Rule of Law Require Judicial Restraint from Expanding the Scope of Blocking Orders Under Copyright Law as an Exceptional Technological Remedy that Directly Impacts Fundamental Rights and the Public Interest

While the Legal Advisor to the Government's position in a precedent-setting proceeding of this type is required to express a balance between the various constitutional rights and public interests involved in expanding the scope of access restriction orders, as a private enforcement remedy against global Internet infrastructure, it is apparent that the normative-legal sources on which it is based are limited to publications or analyses by copyright organizations as interested parties, and all the more so with regard to defining the subjective and objective purpose of Section 53A of the Israeli Copyright Law and the question of the appropriate proportionality of an expansive interpretation of its scope of application.[38]

When the court comes to decide on the plaintiffs' unprecedented request to expand the applicability of Section 53A to a new group of Internet services and infrastructure such as the defendant and DNS Resolver services in general, it is important to examine the public interests related to the granting of the order in a comprehensive view, which requires not only weighing the internal balances within copyright law but also safeguarding fundamental rights, such as freedom of expression, freedom of occupation, the right to privacy, and the right to due process; together with public interests such as maintaining the reliability and proper functioning of the Internet system that operates globally and in a decentralized manner.

Amendment 5 to the Copyright Law established for the first time a new technological remedy of an "access restriction order to a content source," which defines the scope of protection actually afforded to copyright holders, while balancing against the unique dangers of this remedy for unsupervised harm to public rights and interests. As the legal literature notes, one of the central innovations of this proceeding is in making access providers directly involved in resolving the legal dispute between the rights holder and the allegedly infringing website, in a manner that poses a significant challenge to the maintenance of proper judicial review and public oversight.

Thus, for example, the legal literature writes regarding the access restriction order arrangement established in Amendment 5 and underlying the current proceeding: "One of the central challenges associated with granting a technological remedy such as an access restriction order to a content source concerns the principle of the rule of law that underlies our democratic regime, according to which legal liability should not be imposed on a person except by law or by express authorization."[39]

Accordingly, scholars Elkin-Koren and Perel note that the judicial and legislative discussion in the background of the amendment to the law as adopted indicates that its purpose and nature should be defined in a manner that is not focused solely on the need to provide an effective response for copyright holders. That is, alongside the need to ensure effective enforcement of copyright, the need to protect the general public and to protect against over-enforcement of copyrights and the concern for

[38] See for example paragraphs 16, 43, 45-46, 48, 54, 61, which rely exclusively on position papers and reports from copyright organizations.

[39] Niva Elkin-Koren and Ma'ayan Perel, "The Devil is in the Technological Details: On Blocking Orders and the Privatization of Enforcement Following the Copyright Law (Amendment No. 5)" Laws 13, 58-9 (2020). *Attached as Annex 4.*

harm to other fundamental rights such as freedom of expression and the right to privacy must also be considered.

Moreover, the legal literature emphasizes the unique dangers of the order mechanism in terms of the rule of law – and this even before the current attempt to expand it to international actors:

"Due to this uniqueness of access restriction orders, a structural difficulty arises in attempting to subject them to proper judicial review and public oversight. Although the process of issuing orders under the amendment to the law is subject to legal supervision, their implementation, including the definition of technical specifications, is carried out by intermediaries outside the walls of the court. This means that the design of the technological infrastructure necessary for implementing the restriction orders is imposed on access providers that are commercial entities operating to maximize profits, subject to their business discretion. Such private design may be dynamic, biased, and unfair. Without detailed guidance from the court as to what constitutes a proper mechanism for implementing the orders, including what are the most proportionate means of restriction, and without retrospective public oversight of how access was actually restricted, there is a real concern of harm to the rule of law and a sharp deviation from the delicate balance between the protection of copyright and other fundamental rights."[40]

These words, which were written with respect to local access providers, gain even greater force when the expansion of the exceptional liability regime established in Section 53A to infrastructure services at the core of the global Internet is examined, beyond the core and regulated meaning of the term "Internet access providers" in Israeli law. This is the case when there is considerable doubt regarding the institutional capacity of Israeli courts to assess the widespread effects of requested orders with respect to a global service that serves a public far broader than the Israeli public.

D.2 Interpretation of the Term "Access Provider" in Light of the Entirety of Israeli Law on Blocking Websites

The arrangement established in Section 53A does not stand alone in Israeli law. As we shall see below, the expansive interpretation of "access providers" in the copyright law context, as proposed by the plaintiff and supported by the Legal Advisor to the Government, is contrary to the definitions and practice of Internet blocking in Israeli law. In the applicant's view, interpretation of the term "Internet access provider" in the current case must be done also in conformity and harmony with the existing legislative arrangements currently operating in Israel for blocking access to Internet websites, which are applied solely against local ISPs.

In Israel, the legislative framework for judicial orders requiring local Internet access providers to block or restrict access to domain names of websites used for illegal activity was first established in the Powers Law for Prevention of Offenses via Websites, 5777-2017 (hereinafter: the "Powers Law"). This law was enacted following the ruling of the Supreme Court sitting as an Administrative Appeals Court in AAA 3782/12 Commander of the Tel Aviv District of the Israel Police et al. v. Israeli Internet Association, which invalidated the legality of access-blocking orders to gambling websites that the police had issued based on an older authority to close physical gambling premises under the Police Ordinance.

Despite the criminal character of the Powers Law, and indeed because of it, it is a primary and important interpretive source for analyzing the provisions of the legal arrangement and the technological remedy for issuing blocking orders against content sources that infringe copyrights, which establishes in Israeli law the technological and normative distinctions between the different

[40] Niva Elkin-Koren and Ma'ayan Perel, "The Devil is in the Technological Details: On Blocking Orders and the Privatization of Enforcement Following the Copyright Law (Amendment No. 5)" Laws 13, 58-9 (2020). *Attached as Annex 4*, at p. 14.

Internet infrastructures that take part in data traffic between end users and online content, and in which "Internet access provider," "Internet search/location service provider," and "hosting service provider" are distinguished. To the best of the applicant's knowledge, despite the fact that under the Powers Law the state protects significant non-monetary rights, such as the prohibition on prostitution services, terrorism, etc., the state itself has not sought to expand the applicability of orders issued under the Powers Law to free DNS servers of the type operated by the defendant. From a purposive and textual perspective, the Resolver's activity is much closer to the definition of "Internet search/location service provider" in the Powers Law than to the definition of "access provider." Accordingly, an a fortiori conclusion is warranted: if the state chooses not to apply the law to Resolver services in cases of counter-terrorism – where the language of the law allows this with relative ease – there is no justification whatsoever for adopting an expansive and strained interpretation specifically in private copyright enforcement proceedings, where the language of the law supports this far less.
In addition, Israeli law under which Internet website blocking is carried out (including using the terms "Internet access provider" and "hosting service provider") under the Prevention of Harm by a Foreign Broadcasting Body to Information Security Law (Temporary Provision – Swords of Iron), 5784-2024, and the judicial decisions for issuing orders under it, is applied only against local Internet access providers (and against them alone).
If so, these fundamental parts of Israeli law and the entirety of legal thinking in Israel regarding blocking access to websites as a judicial remedy are completely absent from the expansive interpretive move proposed by the plaintiffs and the position of the Legal Advisor to the Government in the current proceeding, and this even when matters of life and death and state security are at stake.
Therefore, in addition to the substantive differences between local ISP services and DNS Resolving services that are globally available, the expansive interpretation of Section 53A as stated should also be rejected on the interpretive ground of harmonization and conformity with the existing legal definitions and judicial proceedings in Israeli law for blocking Internet websites.[]{#_heading=h.or3wjtmg4zh8}

D.3 Comparative Analysis: Normative Distinction Between "Internet Access Providers" and DNS Resolvers

A progressive and consistent international legal trend, evident in case law and legislation in the European Union and other leading democracies, clarifies the necessity of distinguishing normatively and functionally between Internet access providers (ISPs) and services operating in the core layers of Internet architecture.
The leading and primary example of this is the European Union's Digital Services Act (DSA) of 2022, which constitutes the central model today for defining the legal liability of various services in the online space – both toward their users and with respect to illegal content or activity that users may carry out through them. In this regard, the legal framework is based on the distinction between: (a) intermediary services at the infrastructure level (Intermediary Service); (b) hosting services; (c) online platforms; and (d) very large online platforms and very large search engines.
For our purposes, particularly relevant is the internal distinction upon which the legislative provisions are based regarding the legal category of Intermediary Service, which refers to information services provided *on top of* the physical medium supplied by Internet access providers (Internet Access Service) as a separate legal category from them. The recitals to this European Union law unambiguously clarify this distinction:
"Since 2000, new technologies have emerged that improve the availability, efficiency, speed, reliability, capacity and security of systems for the transmission, 'findability' and storage of data online… Such services include, as the case may be, wireless local area networks, domain name system

(DNS) services, top-level domain name registries, registrars, certificate authorities that issue digital certificates, virtual private networks, online search engines, cloud infrastructure services, or content delivery networks, that enable, locate or improve the functions of other providers of intermediary services […] where the communication is delivered via an internet access service."[41]
"[…]Intermediary services span a wide range of economic activities which take place online and that develop continually to provide for transmission of information that is swift, safe and secure, and to ensure convenience of all participants of the online ecosystem. For example, 'mere conduit' intermediary services include generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over IP and other interpersonal communication services…"[42]
It should be clarified that the DSA provisions do not grant an exemption from liability to digital services of this type and even explicitly establish their obligation to act against illegal content on the basis of orders from competent state authorities. However, the legislation reflects a normative change *with respect to the scope and degree of liability of this unique legal category*, which is separate from the established legal categories of hosting services or Internet access services. In other words, the various technological layers of the Internet ecosystem cannot be treated as a single unit, much less in an interpretive exercise.
The DSA reflects the global understanding that the principle of the rule of law and proportionality requires *anchoring in explicit primary legislation* the treatment of the liability regime of infrastructure services available on the contemporary Internet and the cloud computing era, as separate and fundamentally different categories from Internet access providers or the Internet servers connected to them.[43] In our case, a sweeping expansion of the term "access provider" to include Public DNS Resolving services such as the defendant, by way of interpretation or judicial legislation, is contrary to the international trend of regulating the Internet in a precise and proportional manner.
It is further appropriate to refer in this context to the important ruling of the Higher Regional Court of Cologne, which dealt with the very same issue before this Honorable Court, in proceedings brought against the operator of the recursive DNS server Cloudflare. The court held that blocking public DNS servers *is not an appropriate tool for dealing with infringements across the network*. The court noted that Cloudflare's DNS Resolver service constitutes "a tool accessible to everyone free of charge, serves the public interest and participates in a completely passive, automatic and neutral manner in connecting domains on the web." The ineffectiveness of blocking through a public DNS server was also emphasized, since such servers can be switched with great ease.[44]

D.4 Lack of Proportionality of Indefinite Blocking Orders as Harm to Third Parties and Public Resources

We would also like to draw the court's attention to the relevant issue of the time frame for a blocking order in any case of judicial blocking orders against domain names. A domain name has a validity period. The default validity period is usually one year, but a domain name can be registered for longer periods (in Israel, it can be registered for a period of up to five years). When the registration of a domain name expires, it is deleted from the list of domain names distributed to the DNS, and it can be re-registered. Typically, someone who registers a domain name for the purposes of committing an

[41] Digital Services Act, Recital 27.
[42] Digital Services Act, Recital 29.
[43] For further discussion, see above in Parts B and C.
[44] See the extensive publication about the ruling on the Cloudflare website at https://blog.cloudflare.com/latest-copyright-decision-in-germany-rejects-blocking-through-global-dns-resolvers/, *attached as Annex 8*.

offense will not renew its registration if it is blocked (and in the nature of things it will cease to serve its purpose). A blocking order that is not limited in time may therefore harm legitimate domain names that will be re-registered by legitimate parties. Their access will be unlawfully blocked.
If the validity of the blocking order exceeds the domain name's expiration date (or worse, does not determine validity at all) – legal domain names registered by innocent people will be blocked.
Therefore, to the extent that blocking orders are granted as a private remedy under the Copyright Law, the proportionality requirement mandates that the court determine that an access restriction order cannot be valid beyond the expected renewal date of the domain name. This is even more true if the court accepts the position of ZIRA and the position of the Legal Advisor to the Government, and for *the first time* (and *contrary* to the global trend) such orders are issued against global services. These are much further from the public eye than local Internet access providers – so imposing orders on these global services requires extra caution and a different approach.
This principle is also consistent with the position of the legal literature, which emphasizes that technological remedies such as an access restriction order require constant updating and adaptation, and *"one-time legal supervision in advance should not be sufficient, but rather it must be ensured that the benefit of blocking orders compared to their cost and their impact on fundamental rights will also be reviewed retrospectively, in the periods of time after they are issued."*[45]
In this context, the issue of proportionality also requires consideration of the time frame of the blocking order. Granting an order to restrict access without a time limit, or for a period exceeding the validity of the original domain name registration, constitutes a serious violation of the principle of proportionality and creates a real risk of blocking in a scope and extent that exceeds what is necessary. This risk arises because domain names expire cyclically, and may be re-registered by legitimate parties whose access will be unlawfully blocked. This danger gains additional force when the orders are directed at global DNS Resolving services – which are far from public and judicial scrutiny – and require extra caution. Therefore, and in the spirit of the position of the legal literature, the applicant believes that the proportionality requirement mandates that any access restriction order, especially a precedential order directed at global infrastructure, include a limited and predefined validity, as well as a mechanism for periodic judicial review and oversight, as a condition for ensuring the delicate balance between the enforcement of copyright and the fundamental rights of third parties.

Conclusion

The technological and normative differences between Internet access providers (ISPs) that exclusively serve local end customers, and the public DNS Resolving services that are available as global infrastructure for any device connected to the Internet, as detailed in this document, require, in the applicant's opinion, rejection of the expansive interpretation of the term "access provider" in the Copyright Law, and the possibility of issuing access restriction orders based on it against the DNS Resolving service, as proposed by the plaintiffs and the position of the Legal Advisor to the Government.
This proceeding is not personal to Google alone. The decision that will be made within it offers a precedent-setting interpretation and has broad implications for dozens of free and global DNS Resolving services that provide important and critical public value to Internet users in general and in Israel in particular, in aspects of cybersecurity, privacy protection, and global connectivity.
The expansive interpretation proposed by the plaintiffs and the position of the Legal Advisor to the Government of the term "access provider" in Copyright Law is inconsistent with the operation of a free DNS server (resolver) such as the defendant and many others, and the perception emerging from

[45] Elkin-Koren and Perel, supra note 39 and Annex 4, at p. 55.

the documents of the plaintiff and the Legal Advisor to the Government as if free DNS servers are tools whose sole purpose is to access infringing content originates from a narrow and outdated view of the nature of the Internet.

Even assuming that the legislative intent and the language of the legislation in Section 53A does not seek to limit the scope of authority only against Internet access providers as defined in Section 4T(a) of the Communications Law as a service subject to licensing in Israel, no factual foundation or normative justification has been established for the interpretive expansion of the term "access provider" to also include DNS Resolving services operating in the core of the global Internet, given the essential difference between them and local ISP services.

Imposing a blocking order on global DNS Resolving services is not just an extension of legal liability, but a fundamental and dangerous change in the architecture of the global network. It turns a neutral infrastructure that is supposed to serve all users equally into a tool for enforcing local policies, while creating technical inconsistencies and undermining trust in the core systems of the Internet.

List of Annexes

No.	Title	Publisher	Date
1	A Policy Framework for Internet Intermediaries and Content	Internet Society (ISOC)	2025
2	Security and Stability Advisory Committee (SSAC), SAC127 DNS Blocking Revisited	ICANN	2025
3	Security of the Domain Name System (DNS) – An Introduction for Policy Makers	OECD	2022
4	The Devil is in the Technological Details: On Blocking Orders and the Privatization of Enforcement Following the Copyright Law (Amendment No. 5)	Niva Elkin-Koren and Ma'ayan Perel (Laws Journal)	2020
5	Mandated DNS Blocking Critical Considerations	Internet Society (ISOC)	2025
6	DNS at Risk: How Internet Blocking and Fragmentation Undermine the Global Internet	Internet Infrastructure Coalition	2025
7	Policy Brief: Perspectives on Internet Content Blocking	Internet Society (ISOC)	2025
8	Latest copyright decision in Germany rejects blocking through global DNS resolvers	Cloudflare	2023