The Internet Corporation for Assigned Names and Numbers (ICANN)'s response to the Body of European Regulators for Electronic Communications (BEREC) document: "Draft BEREC Report on the Internet Ecosystem"

ICANN is a not-for-profit, public benefit corporation that manages the Internet's unique identifiers. Its mission is to help ensure a stable, secure, and unified global Internet.

ICANN's response to the BEREC document "Draft BEREC Report on the Internet Ecosystem" is limited to the sections relevant to the Domain Name System (DNS).

Measuring the concentration of market forces in the DNS is not a straightforward exercise. The ICANN organization (ICANN org) has many years of experience doing this and would like to contribute the following comments.

DNS Roles: Registration and Operation

One must distinguish between two main areas of the overall DNS ecosystem: registration and operation.

Registration is the process by which a domain name is registered in the DNS. It involves registry operators (top-level domain managers), registrars, and resellers. ICANN org, with the help of the ICANN community, has developed a full set of metrics measuring competition on the registration side. See https://www.icann.org/resources/pages/gds-metrics-en

At the intersection of registration and operation is DNS data publication. DNS data is hosted on "DNS authoritative" servers. Those servers may be operated directly by the domain name owners or by a third-party DNS authoritative server operator. The ICANN Office of the Chief Technology Officer (OCTO) is running a long-term project called the Identifier Technologies Health Indicator (ITHI) which, among other things, is measuring the concentration of third-party DNS authoritative server operators. See https://ithi.research.icann.org/graph-m9.html. A key finding is that the market shares of the different DNS authoritative server hosters depend on the popularity of the domain names. Third-party DNS operators for the top 100 domain names are very different from the one for the top one million.

On the operation side, DNS resolution is typically performed by Internet Service Provider (ISP)-operated DNS recursive servers or public resolvers. The ICANN ITHI project has been measuring and tracking for a number of years DNS recursive server operations. Early work is available at https://ithi.research.icann.org/graph-m5.html. More recently, ICANN org has published a study called "DNS Resolvers Used in the EU" (OCTO-032 https://www.icann.org/en/system/files/files/octo-032-01mar22-en.pdf), which explains the complexities in measuring the actual market share of various operators. It distinguishes between DNS resolvers used by enterprises and cloud services from the ones used by consumers.

One key finding is, as of January 2022: "Within the EU, there is a very distinct difference between consumer and enterprise patterns. Enterprise users use public resolvers in large numbers (39.3%). This is in contrast to consumer use of DNS resolvers in the EU across all ISP sizes: 90.8% of consumers used the DNS resolvers managed by their ISPs in their countries and only 8.5% of them use public resolvers." The second key finding is that numbers relative to consumer usage of public DNS resolvers depend on the size of their ISP: "Only about 4% of consumers served by large EU consumer ISPs are using public resolvers such as Google Public DNS (3%), Cloudflare (0.6%), and Cisco OpenDNS (0.4%)." This study is being extended to cover other parts of the world. Preliminary data is available at https://ithi.research.icann.org/graph-m10.html.

Other Specific Comments on the Report

ICANN org would also like to contribute the following specific comments to the draft report:

Issue 1: See report at p. 16: "The client computers request name translation from a default DNS resolver, which is usually run by the ISP providing the IAS. However, nowadays, encrypted DNS is increasingly used, for example using DNS-over-HTTPS (DoH). This may typically be provided if the web browser sends encrypted requests toward a particular DNS resolver (DoH resolver) which is run by the provider of the web browser, such as Google Chrome or Mozilla."

ICANN org comment: End users have always been able to configure their DNS stub resolvers to point to the DNS resolver of their choice, overriding the default configuration. This was happening long before DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) existed. Note: same comment applies to page 56.

Issue 2: See report at p. 16: "Regarding the domain names stored in the authoritative DNS servers, these are managed at the top level by the international organization ICANN (Internet Corporation for Assigned Names and Numbers). Entities acquiring top-level domain names (e.g. ".com") are called registries. Registries engage with registrars to conduct the business of domain name delegation to users. Many registrars are at the same time also acting as hosting providers."

ICANN org comment: This is an oversimplified view of a complex ecosystem.

Issue 3: See report at p. 47: "Also servicing an authoritative DNS server with a DNS resolver leads to a cost advantage."

ICANN org comment: Best practice is NOT to do this, for security and stability reasons. Also, the cost of running a server on a virtual machine is low, so there is little real savings here.

Issue 4: See report at p. 47: "Large providers relying less on multi-stakeholder processes on definition, introduction and usage of related standards may also be able to pre-set DNS services of many devices and applications, making use of the large user base."

ICANN org comment: Footnote 104 that accompanies the above text in p.47 points back to footnote 102 and is broken. The text referred to in footnote 104 is not included in the document referenced by footnote 102. It might be the case that footnote 102 was changed prior to publication time without updating footnote 104. In any event, the issue described in the above text and in footnote 104 concerns device configuration issues, not multistakeholder processes or standards. While it is true that a resolver - be it an ISP operated resolver or a public resolver, could in theory choose which domains are resolved and could add or remove Top Level Domains while performing resolution, such an activity on a resolver's part would be detected easily by any DNS client verifying the DNSSEC validation signatures. It appears that large public resolver operators do not do such activities.

Issue 5: See report p. 61: "One example is that non-ISP DNS providers might have the incentive to differentiate the way they deal with DNS queries for addresses to their competitors."

ICANN org comment: This could easily be detected if the DNS stub resolver were to verify the integrity of the DNS response using DNSSEC validation; public resolver operators do not appear to be doing this.