ARTICLE 19 response to the Recommendations for ICANN's Root Name Service Strategy and Implementation

Introduction

ARTICLE 19 welcomes the efforts of the Internet Corporation for Assigned Names and Numbers (ICANN) to engage in a multi-stakeholder process by holding this Public Comment Consultation on the Recommendations for ICANN's Root Name Service Strategy and Implementation. [1]

This consultation is an important opportunity, as the rules that ICANN will apply and actions it will take will impact the human rights of internet users. We thus appreciate the opportunity to provide ICANN with our position on the Recommendations for the Root Name Service Strategy and Implementation and we look forward to the discussions that will follow.

This statement is made on our own behalf. We also endorse comments by the Non Commercial Stakeholder Group (NCSG) and those of the At-Large Advisory Committee (ALAC).

About ARTICLE 19

ARTICLE 19 is an international human rights organisation that works to protect and promote free expression, which includes the right to speak, freedom of the press and the right to access information. With regional programmes in Africa, Asia, Europe, Latin America, and the Middle East and North Africa, we champion freedom of expression at the national, regional, and international levels. The work of ARTICLE 19's Digital Programme focuses on the nexus of human rights, Internet infrastructure, and Internet governance.

At ICANN, we engage through the ICANN Empowered Community as members of the Generic Names Supporting Organization (GNSO) under the Non-Commercial Users Constituency (NCUC) and as members of the At-Large Advisory Committee (ALAC) directly as part of the European Regional At-Large Organization (EURALO). We work within the ICANN community with the main purpose of raising awareness of how the Domain Name System (DNS) affects human rights. This aim would ensure that Section 27.2 of ICANN Bylaws (on Human Rights) and other Bylaws with an impact on Human Rights are implemented in full and put the user at the centre of policy development processes.

1 Recommendations for ICANN's Root Name Service Strategy and Implementation <https://www.icann.org/public-comments/root-name-service-implementation-2020-10-27-en> accessed 05 December 2020

Summary

On 26 October 2020, ICANN, through the Office of the Chief Technology Officer (OCTO), published the Recommendations for ICANN's Root Name Service Strategy and Implementation, seeking input from the community. In December 2020, ARTICLE 19 reviewed the ICANN Recommendations for ICANN's Root Name Service Strategy and Implementation.

The document describes, at a high level, the ICANN organization's strategy and implementation plans for the ICANN Managed Root Server (IMRS). It envisages a multipronged strategy that expands and enhances existing approaches and facilitates the standardization and implementation of technologies such as Hyperlocal, which seek to improve the decentralization of the root name service to mitigate risks that the RSS may face over time.

Though it's important to uphold and protect the confidentiality, integrity, and availability of the Root Server System (RSS) during attack, apt measures, processes, and steps in compliance with human rights must be put in place.

Our analysis shows that the draft contains several positive and commendable provisions, including the involvement of every stakeholder, the intention to expand and place root server instances in diverse locations, and information sharing through training and capacity building to encourage DNSSEC validation.

However, the recommendations do not fully address the human rights implications of the recommendations, as they propose data monitoring but do not provide clear guidance on its scope and limitations, place privacy concerns on the back burner, and do not envisage implementation of the recommendations of the 2019 ICANN Human Rights Impact Assessment report[2].

While we are aware of the growing volumes of traffic generated by legitimate users of the global Domain Name System (DNS), driven by many factors such as the growing number of new Generic top-level domains (gTLDs), the steady increase in the complexity of web pages with embedded domain names, and the growing number of connected devices that perform DNS queries, ARTICLE 19 does not believe that these complexities absolves OCTO of its responsibility to sufficiently address the human rights implications.

ARTICLE 19 therefore urges OCTO to consider the recommendations below, which would help align the Recommendations for ICANN's Root Name Service Strategy and Implementation more closely with international law and best practice.

2 Summary report of the first Human Rights Impact Assessment for the ICANN organization <https://www.icann.org/en/system/files/files/summary-report-hria-15may19-en.pdf> accessed 05 December 2020

Placing of Root Server Instances in Diverse Locations

We commend the high-level goal of making new IMRS single instances available at a low initial cost to organizations that have good connectivity. We also welcome the recent IMRS cluster launched in October 2020 in Singapore (making it ICANN's first in the Asia-Pacific region).

While we appreciate that it might be resource-intensive to adopt IMRS single instances and clusters in varied geographical locations, it is important to highlight the need to increase geographic representation, particularly for underserved regions. We note that more IMRS instances and clusters would enable more of the DNS queries originating in these underserved regions to be answered much faster, regardless of the behaviour of networks or servers in other regions.

Increased IMRS single instances and clusters would therefore markedly increase the quality of information access and dissemination for people and communities that are often least represented in internet governance and therefore disproportionately lack high-quality infrastructure. We thus welcome these steps and recommend that this support for new IMRS instances should focus on underserved regions as the first priority.

Data Protection, Privacy, and Confidentiality

We concur with the statement, '*Confidentiality attacks aim to expose sensitive information*.' under Section 4.3. We also welcome the recognition that the original DNS protocol suite transmits and receives data without encryption and that backward compatibility from unencrypted DNS to encrypted DNS has often been challenging. The potential for information leakage could lead to serious breaches of confidentiality and, as a result, users' privacy.

We thus recommend that more effort and resources be dedicated and directed towards coordination with the Adaptive DNS Discovery (add) and DNS PRIVate Exchange (dprive) Working Groups of the Internet Engineering Task Force (IETF). The two groups are focused on providing technical solutions related to the discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs; supporting both encrypted and unencrypted resolvers; and working on mechanisms that increase the confidentiality of the DNS.

Given that the scope of the two groups is limited to developing technical mechanisms, the Recommendations for ICANN's Root Name Service Strategy and Implementation should explicitly mention coordination with the two Working

Groups. Additionally, ICANN can adopt the mechanisms of the two IETF Working Groups into policy recommendations, which should be subject to the standard ICANN Policy Development Processes.

Enhancing Root System Monitoring

We recognize that malicious actors use the DNS as a tool to perpetrate criminal and unlawful activities. However, we strongly oppose the proposition to develop and deploy monitoring systems as proposed in Section 3.2. The use of network active probes is in blatant defiance of and disregard for freedom of expression and information. Monitoring, if used at all, should only be undertaken in response to complaints of alleged violations of Terms of Service and subject to publicly available transparency reporting, independent oversight, and access to remedies as explicitly set out in international human rights standards. Baseless monitoring creates an environment of surveillance, which not only threatens users' right to privacy, but may also contribute to a chilling effect on freedom of expression online, as internet users may choose to self-censor or refrain from online participation altogether. .

The United Nations Special Rapporteur on freedom of opinion and expression expressed similar concerns in his 2016 report, in which he states that this chilling effect is "*a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children*."[3]

Investigation into IMRS Cloud

As proposed under section 4.1.1, ICANN should extensively investigate the cloud services landscape and potential costs associated with the use of cloud services as a solution for increasing the number of IMRS instances. However, any eventual use of these services can create potential human rights concerns, especially if contracted third-party cloud providers do not have consistent, transparent, and user-centric policies on handling DNS query data.

ICANN should clearly and explicitly include human rights considerations, including strong data protection requirements, through contracts with any third-party personnel engaged in the cloud landscape. This will help ensure that internet users' privacy and security are considered in all IMRS Cloud policies.

3 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 May 2016.

Conclusion

ARTICLE 19 is grateful for the opportunity to engage with ICANN in this process, in light of the five objectives under ICANN's Strategic Plan for Fiscal Years 2021-2025.

We look forward to continued collaboration to strengthen human rights considerations in the Domain Name System and particularly in ICANN's policies and procedures. We welcome further engagement opportunities and avail ourselves in case of any questions or concerns.

If you would like to discuss this analysis further, please contact Ephraim Percy Kenyanito, Senior Digital Program Officer, at ephraim@article19.org. Additionally, if you have a matter you would like to bring to the attention of the ARTICLE 19 Digital Programme, you can contact us by e-mail at digital@article19.org.