ARTICLE 19 response to the Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2

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 Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2. [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 Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2 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

1 Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2 <https://www.icann.org/public-comments/policy-recommendations-epdp-phase-2-2020-12-03-en> accessed 15 January 2021

ensure that Section 27.2 of the 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.

Summary

On December 3 2020, ICANN published the Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2, seeking input from the community. In January 2021, ARTICLE 19 reviewed the Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2.

The Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2 provides recommendations on how Registries and Registrars will handle registrant data in light of the European Union's General Data Protection Regulation ("GDPR").

Our analysis shows that the draft contains several positive and commendable provisions, including allowance for proxy registration.

However, it does not fully address the human rights implications of the recommendations, which propose mass data retention and publication of users' city data but do not provide clear guidance on their scope and limitations and place privacy concerns on the back burner.

ARTICLE 19 therefore urges ICANN to consider the recommendations below, which would help align the Recommendations for Final Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2 more closely with international law and best practice.

Recommendation #19:

While we appreciate that the Recommendation provides an opportunity for domain name registrants to use privacy/proxy services in order to mask registrant data, it is important to highlight that the last sentence as phrased negates the entire purpose of the PDP process, as it states, "*The full privacy/proxy RDDS data may also include a pseudonymized email.*" This is the same case in the implementation notes, which state, "*The intent of this recommendation is to provide clear instruction to registrars (and registries where applicable) that where a domain registration is done via an affiliated and/or accredited privacy/proxy provider, that data MUST NOT also be redacted. The working group is intending that domain registration data MUST NOT be both redacted and privacy/proxied.*"

The EPDP has defined pseudonymized email as "*the same unique string [...] used for multiple registrations by the data subject*". Essentially, this requirement makes the

pseudonymized email address a unique identifier that undermines the very protection of pseudonymization. Whereas it may be difficult to identify a registrant on the basis of a single registered domain name, the fact that multiple domain names registered by the same person can be linked to each other increases the potential that the registrant can be easily identified. This threat to anonymity not only constitutes a threat to registrants' privacy, but may also contribute to a chilling effect on individuals that must disseminate information anonymously, particularly those that are marginalised or under threat by government actors for their speech.

We recognize that public availability of registrants' unique pseudonymized email undermines freedom of expression and information. Therefore, the recommendation should be redrafted to make it MANDATORY that no pseudonymized email will be publicly published without a registrant's express and informed consent.

Recommendation #20:

We recognize that the EPDP Team recommends that the previously concluded EPDP Phase 1 Recommendation #11 has been updated in Recommendation #20 to state that redaction MAY be applied to the city field in reference to the registrant's contact information, instead of MUST. However, we strongly oppose this proposition as the Recommendation allows for registrant location data to be publicly accessible to anyone, regardless of legitimate interest. Similar to Recommendation #19, the public availability of registrant location data compromises freedom of expression and information.

In a 2015 letter to the then ICANN CEO Fadi Chehade, former Congresswoman Katherine Clark pointed out[2] the danger of the then WHOIS system as it then was as it had been used by "*..abusers to orchestrate an online intimidation tactic known as "doxing…The incidents range from online abusers' attempts to send SWAT teams to break into women's private residences, to women fleeing their homes after receiving specific violent threats including their address or photos of their homes…..*". Additionally these concerns were shared by an alliance of digital rights groups, anti-harassment initiatives, media advocacy groups, women's rights organizations, and private individuals in a 2015 letter to ICANN[3].

The publication of city information of a registrant of a domain name makes it much easier for malicious actors to continue engaging in the manner described above, as easy access to this type of information makes it easier to extend their threats

2 Senator Katherine Clark July 6, 2015 letter <https://drive.google.com/file/d/0B-QkCUPMetwXQVVOVHNQX1luQ1k/view> accessed 21 January 2021

3 Letter to ICANN <https://www.apc.org/sites/default/files/Letter%20to%20ICANN_0_0.pdf> accessed 21 January 2021

offline. This 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 this kind of online participation altogether.

In this regard, ICANN should clearly and explicitly make it MANDATORY that redaction of city information should be applied. This will help ensure that internet users' privacy and security are considered in all domain registration policies.

Recommendation #21:

We welcome the attempt at including a maximum data retention period as stated in Recommendation #21: "*registrars MUST retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months.*" However, we note that there is a sentence at the end of the recommendation that potentially renders the recommendation moot, as it states, "*For the avoidance of doubt, this retention period does not restrict the ability of registries and registrars to retain data elements for longer periods.*"

Data retention ought to be practiced only when it is necessary to do so, as keeping large troves of data poses risk in managing its security and confidentiality. Given that the EPDP is an attempt to ensure compliance with the GDPR, it is important to note that mandatory mass data retention was deemed to be unlawful in December 2016 by the Court of Justice of the European Union (CJEU) through two cases: *Joined Cases Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v. Watson*[4]. Though the rulings were about communication metadata, the court found that mass data retention can allow for profiling of individuals, which is incompatible with Article 7 and 8 of the EU Charter of Fundamental Rights.

In this regard, ICANN should clearly and explicitly make it MANDATORY that data is retained only for the minimum time frame necessary for its clearly stated purpose of use, especially where a user has expressly terminated domain services. Additionally, the recommendation should be redrafted to ensure that all DNS actors that handle registrant data are transparent and accountable to registrants as to how they handle the data retained and should notify them and provide remedies in case of any data breaches or leaks. This will help ensure that internet users' privacy and security are considered in all domain registration policies.

4 Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson <https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/> accessed 15 January 2021

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.