

Comments to the ICANN Generic Names Supporting Organization on the Privacy & Proxy Services Accreditation Issues Policy Development Process Working Group Initial Report

July 7, 2015

Dear members of the Generic Names Supporting Organization,

We wish to express our concern over the Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process, which includes recommendations for the accreditation of Privacy and Proxy Service Providers (PPSPs). The report noted that some members of the Privacy & Proxy Services Accreditation Issues Working Group supported a recommendation that would force PPSPs to disclose their customer's personal information without legal due process.

[Access](#) is an international organisation which defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all. We believe that a secure internet is critical to defending and extending the digital rights of users around the world, especially the right to privacy, association, and freedom expression. Our Technology Arm supports human rights defenders and organizations via a Digital Security Helpline, participates in the development of secure communications tools, and helps inform the broader human rights and digital security community through our research and analysis.

The implementation of some of the policies described in the report would result in harmful consequences for user privacy. ICANN manages resources that users all around the world rely on for the exercise of their rights. Below, we summarize the concerns so that the GNSO Council, the ICANN Board, and all stakeholders involved in this policy development process will consider taking actions to ensure the respect of basic human rights such as the right to privacy.

- **Human rights, due process, and user data disclosure:** In order to comply with human rights standards¹, any rules forcing PPSPs to disclose or publish user data upon request must comport with legal due process and require a court order or a subpoena for its execution whether the requestor is a private party or a law enforcement authority². Mechanisms for user data disclosure that do not comply with due process or which put excessive burdens³ on PPSPs endanger freedom of expression by exposing users at risk – such as activists, members of ethnical, religious or sexual minorities, journalists and others – and human rights groups that protect those users.
- **Policies must consider the universal scope of human rights:** The most protective approach towards user privacy must be adopted in the case of any gaps between between domestic legislation and international human rights standards.
- **Impact on ICANN policies on companies seeking to protect human rights:** As private companies, PPSPs also have a duty to comply with human rights standards, including the protection of privacy and due process. ICANN - itself a private entity - should avoid the imposition of excessive burdens that may discourage PPSPs lawful activities.
- **Ensuring civil society groups and activists can continue using PPSPs:** PPSPs can be crucial to actors working to help protect human rights defenders and groups that work with digital users at risk. Any policy development work in this area - including discussions of restrictions on “commercial” usage of PPSPs - must be carefully undertaken in order to ensure there is no negative impact on the lawful usage of such services by civil society organisations, public interest groups, individual activists, and whistleblowers.

¹ Like the International Principles on the Application of Human Rights to Communications Surveillance and its Implementation Guide, among others. See <https://en.necessaryandproportionate.org/> and <https://www.accessnow.org/blog/2015/05/03/access-releases-implementation-guide-surveillance-necessary-proportionate> respectively.

² Pages 12 and 13 of the report, numbers 18 and 19: [...] *the WG agreed that none of its recommendations should be read as being intended to alter [...] the prevailing practice among P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a P/P service customer. It also notes that disclosure of at least some contact details of the customer may in some cases be required in order to facilitate such direct resolution. / The WG has developed an illustrative draft Disclosure Framework that would apply to Disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners. The proposal as drafted includes requirements concerning the nature and type of information to be provided by a Requester, non-exhaustive grounds for refusal of a request, and the possibility of neutral dispute resolution/appeal in the event of a dispute [...]*

³ Some of the proposed rules on relaying third party requests put excessive logistical and economic pressure on PPSPs. See page 11 on the report, numbers 16 and 17.

- **Intermediary Liability Limitation:** Even in the cases where the registration of PPSPs was imperative, the policies set in place by ICANN should provide the necessary safeguards to allow them to conduct legal business and to limit their responsibility for the acts of their users beyond their control as Internet intermediaries.

In addition to the remarks in this brief, we support the concerns raised by the Online Abuse Prevention Initiative in an open letter that is being addressed to the ICANN⁴.

Contact Information:

Javier Pallero

Policy Analyst

javier@accessnow.org

Raman Jit Singh Chima

Policy Director

raman@accessnow.org

⁴ The letter can be found here <http://onlineabuseprevention.org/letter-to-icann-july-2015/>