CONSIDERING THE RESPONSE OF NCSG TO THE DETAILED QUESTIONS ASKED OF SG'S BY THE PROXY/PRIVACY ACCREDITATION WORKING GROUP

ALL NCSG MEMBERS OF THE PPSAI INCLUDED ALONG WITH OFFICERS OF NCSG. PLEASE FEEL FREE TO ADD MORE PEOPLE TO THIS DRAFTING SESSION. TX!!!

Stakeholder Group / Constituency / Input Template

Privacy & Proxy Services Accreditation Issues PDP Working Group

PLEASE SUBMIT YOUR RESPONSE AT THE LATEST BY **[To be confirmed – minimum of 35 days]** TO THE GNSO SECRETARIAT (gnso.secretariat@gnso.icann.org), which will forward your statement to the Working Group.

The GNSO Council has formed a Working Group of interested stakeholders and Stakeholder Group / Constituency representatives, to collaborate broadly with knowledgeable individuals and organizations, in order to consider recommendations in relation to Privacy & Proxy Services Accreditation Issues.

Part of the Working Group's effort will be to incorporate ideas and suggestions gathered from Stakeholder Groups and Constituencies through this template statement that contains questions that the GNSO asked the WG to address. Inserting your responses in this form will make it much easier for the WG to summarize the responses. We have categorized the items in the hope that it adds clarity.

This information will be helpful to the community in understanding the points of view of various stakeholders. Please answer as many questions as you can. In addition, please feel free to add any information you deem important to inform the Working Group's deliberations, even if this does not fit into any of the questions listed below.

A short list of definitions that the Working Group hopes your Stakeholder Group/Constituency will find helpful follows after the list of questions. For further information, please visit the Working Group's Workspace (see https://community.icann.org/x/9iCfAg).

Questions from the Working Group Charter:

I. MAIN ISSUES

1. What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?

2. Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?

Yes, ICANN should definitely distinguish between privacy services (which identify the registrant and serve as a forwarding address) and proxy services (which do not identify the registrant).

3. What are the contractual obligations, if any, that if unfulfilled would justify termination of customer access by ICANN-accredited privacy/proxy service providers?

"Customers" are of course, domain name Registrants, and we think that whatever the terms of the contract are with the Registrant should govern the existence or termination of the service. Consent of the Registrant should, of course, be informed. Termination should include multiple options, including "Takedown" in lieu of "Publication."

4. What types of services should be covered, and would be the forms of non-compliance that would trigger cancellation or suspension of registrations?

This should be subject to the contracts and relationships of the proxy/privacy service providers and their customers. It's a Market Issue, not an ICANN issue. We note that Registrars should be encouraged to have customer-supportive (as opposed to customer-hostile agreements).

5. What are the effects of the privacy and proxy service specification contained in the 2013 RAA? Have these new requirements improved WHOIS quality, registrant contactability and service usability?

We would need concrete data and research provided to the WG because this are terms newly adopted and their implementation results are not yet publicly known.

6. What should be the contractual obligations of ICANN accredited registrars with regard to accredited privacy/proxy service providers? Should registrars be permitted to knowingly accept registrations where the registrant is using unaccredited service providers that are however bound to the same standards as accredited service providers?

Private proxies, e.g., attorneys, have always been deemed hard to identify, and we do not see how that will change. Attorneys will always assert Attorney-Client Privilege and defend the confidentiality of the

businesses or organizations or individuals they represent.

But knowing this practice is going on widely in the background, for those who can afford this high level of protection, should inform the discussion and debate of other smaller groups and businesses seeking a similar service.

Some within the NCSG strongly support the policy that Registrars accept registrations from those Not Bound to the accreditation standards; others feel that such a policy may be inadvertently unavoidable (as when a son or daughter registered a domain name for a senior parent), but that Registrars working with proxy/privacy service providers on a large scale or a formal scale should be accredited.

ICANN already distinguishes between *Privacy Services* and *Proxy Services*. A privacy service applies to the entity (or human) to allow alternate but valid means of identification. A Proxy Services applies more to the product directly (the domain name) relating back to the public Whois information: the proxy service becomes the lawful surrogate of registration. (http://www.icann.org/en/resources/compliance/complaints/whois/privacy-proxy-registration)

II. MAINTENANCE

1. Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?

Some in the NCSG believe that affiliated proxy and privacy services should identify themselves; some do not.

The WG would need to announce "for what purpose" that identification was being requested since many companies, organizations and individuals register domain name through third parties, including web host providers, website designers and lawyers.

Requesting of "labeling" of privacy services should not be subject to vague or generalized reasons such as improvement of services or to help prevent fraud and abuse. The idea that all who seek anonymity are typically involved in crime is totally unsubstantiated.

2. Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?

The accuracy of the Registrant Whois data held by the Proxy and Privacy Service Providers should be no different in the validation or verification than what is required by the 2013 RAA. The choice of confirming an email or telephone number, at the choice of the Registrar's Accredited Proxy or Privacy Service Provider - and serves the same purpose, namely the reachability of the Registrant in the case of

technical problems with the domain name.

3. What rights and responsibilities should customers of privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.

Customers/Registrants should have the rights and responsibilities as set out in their agreements with their proxy or privacy service providers. They should have the rights and protections of privacy and due process as afforded by national laws and incorporated into the Service Providers contract.

4. Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?

ICANN-accredited privacy/proxy service providers should absolutely not distinguish between domain names used for commercial vs. personal purposes. The Whois Review Team found that Registrants of all flavors - commercial, noncommercial and individual - use proxy/privacy registrations for very needed and legitimate services including protection of home addresses (individuals), protection of the location of a dissident group or religious minority institution (organizations), and prior to the unveiling of the new name after a merger, a new movie title, or other types of new products and services, including during the long months between finding the name, preparing the advertising and marketing plan, and then launching (companies).

Thus, as found by the Whois Review Team and every Task Force that has ever looked at this issue in ICANN, the use of proxy/privacy registrations for use by ALL REGISTRANTS is appropriate, of course and including commercial purposes (whatever that may mean), and no gates or classes should be imposed, installed or built.

5. Should there be a difference in the data fields to be displayed if the domain name is registered or used for a commercial purpose, or by a commercial entity instead of a natural person?

We can think of no reason whatsoever to impose additional fields on the millions of noncommercial organizations, home-based businesses (of seniors, mothers, and others), and individuals based on the purpose to which they may devote (or not devote) their domain name now and in the future. It is a content issue far outside the limited technical scope and reach of ICANN. We can provide much more data on this issue as it arises in the WG, should it be needed.

6. Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

Again, absolutely not. Domain names are domain names, and their use by noncommercial organizations, hobby groups, public interest groups, religious organizations, charity groups, educational organizations,

research groups -- as well as entrepreneurs, small businesses and individuals -- should not be barred or limited in any way. As the Whois Review Team found, all of these groups use proxy/privacy services - and have legitimate reasons for doing so.

For those small number of "public trading companies," in which there is an exchange of goods and services with the public (and that is very, very small percentage of businesses online), national and regional laws should apply -- as having a public "storefront" invokes not ICANN rules, but local laws.

III. CONTACT

1. What measures should be taken to ensure contactability and responsiveness of the providers?

The RAA raises some good ideas. We would like to talk in the WG with the P/P Service Providers to see what they think, how the new rules are working, and whether they serve the purpose for which they were intended (contactibility of the proxy/privacy service provider).

2. Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?

Again, we refer back to the 2013 RAA and call on those who have implemented and oversee compliance with these provisions (both Registrars and ICANN Staff) to share what is happening and how things are proceeding.

3. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?

We would be interested in hearing any concerns that might be raised by the privacy/proxy service providers about this recommendation.

4. What are the forms of alleged malicious conduct, if any, that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?

This question is ambiguous. We assume this question refers to alleged misconduct by the proxy/privacy service provider, and call on the WG to discuss when and how the proxy/privacy service provider must respond or be able to restrict inquiries -- especially when coming from a) known bad actors (e.g., people intentionally and purposely harassing a organization over its ideas, orientation or purposes, b) frivolous actors (e.g., those known for harassing competing businesses or other groups and individuals without basis), and other reasons for rejecting or ignoring ill-intentioned, bad faith or ultra-voluminous requests or demands by third parties for proxy/privacy service resources.

IV. RELAY

1. What, if any, are the baseline minimum standardized relay processes that should be adopted by ICANN-accredited privacy/proxy service providers?

Requests and demands for relay can be generated by spam or electronic means as easily as anything else. We support the imposition of reasonable efforts by proxy/privacy service providers to ensure that the requests being relayed are genuine, in good faith and not repetitive.

2. Should ICANN-accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?

Absolutely not. As set out above, these allegations can be illegitimate, generated by spam, or simply coming from well-known bad actors. Further, the same requestor can be harassing a particular religious group for its messages, or a particular individual for reasons equivalent to cyber-stalking. Proxy/privacy service providers should have it within their discretion and terms of service to accept and/or reject allegations that seem to be illegitimate, harassing, potentially illegal, or simply too voluminous and repetitive. We look forward to talking with the WG's P/P service providers about their screening mechanisms for good faith and non-repetitive allegations of illegal activities.

V. REVEAL

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?

NCSG respectfully submits that "reveal procedures" should be subject to legal processes as defined by the jurisdiction of the proxy/privacy service providers. What is illegal in one country is not illegal in another country, e.g., calls for the "outing" of pro-democracy groups in the US and registered through a US proxy/privacy service provider by Chinese law enforcement should be clearly subject to and worked through international law enforcement mechanisms - which have long existed and are under further revisions and development in cyber-treaties of many types.

Reveal policies regarding privacy/proxy services should not threaten fundamental freedoms, such as freedom of expression. Requests for "reveal" should not be automatically associated with crime, but rather should be primarily understood as a threat to the preservation of registrants' privacy as noted by the Universal Declaration of Human Rights.

2. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of ensuring timely service of cease and desist letters?

There is no requirement that a "Cease and Desist" letter sent by a private attorney on behalf of

his/her/its client be accurate or independently reviewed. In the real world, one attorney generally sends a "Cease and Desist" letter to another and that attorney evaluates whether it is a) Frivolous and needs to response, b) Legitimate and meriting a response, or c) shows that the other side is actually the "Junior User" and infringing on the recipient's trademark, at which point the attorney may send back a "Cease and Desist" letter on behalf of his/her/its client.

Cease and Desist letters, however, should certainly be passed on to Registrants (provided they have not been sent numerous times), and thus this issue should be moved to IV, Relay, above.

3. What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger such disclosure? What specific alleged violations, if any, would be sufficient to trigger such publication?

NCSG respectfully submits that the proxy/privacy service provider should have the discretion pursuant to its contract to set the terms of its disclosure. Should the p/p service provider choose to operate in compliance with its national law and require a court order -- and the independent judgment of a judge, magistrate or other judicial authority that an identity should be revealed -- that is a decision ICANN must uphold and endorse.

4. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?

NCSG submits that this question is the real core of the issue that the WG should be evaluating. How can we protect Registrants engaged in Free Speech/Freedom of Expression - as well as those introducing competition to well-established entities - as well as those seeking privacy for their location (from harassment or stalking regardless of the message they deliver online)?

One address disclosed to the wrong party can be one person's life (see California Department of Motor Vehicles which disclosed the name and address of a young celebrity through a process of disclosing driver's license information to those who requested it in person, and the young celebrity was stalked and killed at her home).

This is the key question of the reveal process. Proxy/privacy service providers must be allowed to operate subject to the protections and requirements of national law - lest they become responsible or liable for kidnappings, dangers, harassment and worse. This is an area where the WG and ICANN must be supporting the proxy/privacy service providers and their knowledge and operation under national law and in correspondence with national courts.

We see no way that the WG could urge otherwise - and thus expose the p/p service provider to liability and risk. Further, it is consistent with the expectations of a Registrant, e.g., a Human Rights Organization, who will choose the location of its Registrar and its Accredited P/P Service Provider, e.g, in Canada, knowing the protections of the Canadian law for human rights.

5. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?

There are very few safeguards AFTER an address is released and a minority religious group, or a home-based business exposed. The best alternative, as discussed in the WG, is to allow a "rapid takedown" of the domain name (together with its emails, websites and listservs) prior to Reveal, if the Registrant request. Otherwise, Reveals subject to the due process mechanism of the proxy/privacy service provider should supporting by the WG.

A process of administrative and judicial redress would be appropriate in this case to guarantee that all care is taken into consideration.

6. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?

Warrants and subpoenas under local law and other forms of compliance with the Due Process standards of local law of the Registrar and its Accredited P/P Service Provider.

7. What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access (if such access is warranted)?

The circumstances would have to be delimited by a process of safeguards. To protect registrants, access to private information would have to be granted by a well-structured procedure subject to proportionality, data minimization, and unambiguous objectives.

Other information/Suggestions:

NCSG respectfully submits that the PPSAI has at least two additional questions it should be looking at:
1) What safeguards must be put in place not only to ensure adequate protections for privacy and freedom of expression, but to ensure protection of individuals, noncommercial organizations and even companies from **anti-competitive activity** (those using the Whois data to threaten a competitor, often smaller, to drive away competition) and from **personal injury** (those using Whois data as a locator to find someone running a home-based business, controversial organization or an disliked individual to intimidate, hurt or stalk them or their families)?

Overall, NCSG submits that this WG has an obligation to expand the forms of abuse it is looking at to the full range: to the harassment of groups, organizations, individuals and businesses for the ideas they espouse or the goods that they sell. Reasons for seeking proxy/privacy services include the need to protect one's ideas (from persecution, informal or state-ordered), to protect one's goods or services

(from anticompetitive activity), and to protect one's person (from harassment and stalking, perhaps unrelated to any communication via or in conjunction with domain names).

To that end, this WG should be examining the Abuse of Whois Data that we know, that have been studied and discussed in GNSO Studies and Task Forces since the beginning of time, and finding ways protect new and future Internet users - now approaching 2 Billion.

2) What threshold should be put into place to ensure that an allegation is not an unfounded accusation?

An allegation or accusation by an attorney or law enforcement (absent a warrant or subpoena) is not a trial or independent determination. A due process mechanism, probably different for different type of accusations and accusers, should be implemented. We recognize that that Proxy/Privacy Providers will make these decisions together with their attorneys and consistent with their national laws.

3) What additional options must be included in this WG's evaluation of alternatives should someone seek the information of a customer of proxy/privacy services - a Registrant?

NCSG respectfully submits that "takedown" should be an option by those proxy/privacy service who elect to offer it. Rather than a reveal that might expose proxy/privacy service providers to some form of blame or liability (see #1 in this section above for misuses of Whois data, including those that cause damage to persons and businesses), some p/p providers may choose to offer their customers a "takedown" option - to lose the domain name (and its websites, listservs and emails) rather than relinquish their privacy.

This concept was discussed in the WG and has received sufficient support to merit its inclusion in future WG and ICANN discussions and decisions.

****

LIST OF RELEVANT DEFINITIONS

(1) Privacy & Proxy Services

The following definitions are those used by the GNSO in the various WHOIS studies that it commissioned between 2010-2012 (http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf):

- ***Privacy services*** hide customer details from going into WHOIS. Privacy service providers, which

may include registrars and resellers, may offer alternate contact information and mail forwarding services while not actually shielding the domain name registrant's identity. By shielding the user in these ways, these services are promoted as a means of protecting personal privacy, free speech and human rights and avoiding personal data misuse.

- ***Proxy services*** protect users' privacy by having a third-party register the name. The third-party is most often the proxy service itself. The third-party allows the user to access and use the domain name through a separate agreement or some other arrangement directly with the user. Proxy service providers may include web design, law, and marketing firms; web hosts, registrar subsidiaries, resellers and individuals.

NOTE: The 2013 Registrar Accreditation Agreement contains a temporary specification relating to Privacy & Proxy Services (http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.pdf), which refers to these services as follows:

1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.

1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (Whois) or equivalent services.

1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (Whois) or equivalent services rather than the P/P Customer's contact information.

1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

(2) Relay & Reveal Requests

The following descriptions are taken from the GNSO's Terms of Reference for a proposed Proxy & Privacy Relay & Reveal Study in 2010 (http://gnso.icann.org/issues/whois/whois-proxy-privacy-relay-reveal-studies-tor-29sep10-en.pdf):

- For many domains, Registered Name Holders can be reached directly at addresses obtained from WHOIS. However, for Privacy/Proxy-registered domains, Registered Name Holders or third party licensees cannot be reached directly via WHOIS- published addresses. Instead, ***communication relay requests*** may be sent to the Privacy/Proxy service provider published in WHOIS, or attempted using addresses obtained from other sources, websites or communications associated with the domain.
- For many domains (including those registered via Privacy services), the Registered Name

Holder's identity is published directly in WHOIS. However, for domains registered via Proxy services, the name of the licensee is not published in WHOIS; third party licensees can typically only be identified by ***asking the Proxy to reveal the licensee's identity***, given reasonable evidence of actionable harm.