**GROUPING OF CHARTER QUESTIONS (WITH ADDITIONAL SUGGESTIONS)**

**As of 16 January 2014**

**Note:**

* **Framework/grouping used here is that suggested by Jim Bikoff**
* **Bullet points in italics attempt to summarize/note questions and suggestions from various WG members relating to either clarification of/adding questions**

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

* *Consider a “take down” of the domain name as an option*
* *Consider customer option for different methods and notification issues*

1. What types of services should be covered, and would be the forms of non-compliance that would trigger cancellation or suspension of registrations?
2. 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?

* *Postpone this discussion given that the RAA only went into effect on 1 Jan 2014?*

1. 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?

**II. MAINTENANCE**  *(OR REGISTRATION?)*

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?
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?

* *What is the RAA’s current requirement on this point?*
* *How would such checks be conducted and by what means?*

1. 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.

***Basic Registration Issues***

1. Should ICANN-accredited privacy/proxy service providers distinguish between domain names used for commercial vs. personal purposes?

* *Any difference between “personal” vs “noncommercial” e.g what about noncommercial organizations?*

Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes?

* *Consider protections for noncommercial organizations such as political, hobby, religious and ethnic groups*
* *What about domain names affiliated with or controlled by a P/P service?*
* *Must P/P services disclose affiliated interests?*

1. 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?

* *Registration AND (not OR) use?*
* *Is this within ICANN scope/mission?*
* *How to deal with noncommercial organizations that may be incorporated as corporations for insurance or liability purposes?*

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

* *Why not also organizations and non-profits?*

**III. CONTACT**

1. What measures should be taken to ensure contactability and responsiveness of the providers?
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?
3. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
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?

* *Difference between “illegal” and “malicious”?*
* *Need protections for free expression, privacy, legitimate competitive activity, stalking, harassment and abuse?*

**IV. RELAY**

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

* *Plus publication of email address?*
* *Any difference if enquiry is from law enforcement or not, e.g. attorneys or others?*
* *Does it matter where the enquiry originated? Should country where the activity was supposed to have occurred matter? Any difference if P/P service is in a different jurisdiction? Any difference if activity is illegal in one jurisdiction but not the other (e.g. if P/P service is in jurisdiction that provides additional defense/protection whereas the originating country does not)?*
* *If allegations are received from supposed victim, how to protect her safety/privacy? Require redacted requests?*
* *Should P/P service have discretion to forward rather than be mandated (outside a court order)?*

**V. REVEAL**

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

* *And also require notification of the customer?*

1. 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?
2. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?

* *Other concerns include anti-competitive activity, stalking/harassment and other motives unrelated to the purpose of the domain name*

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

* *Not just published but revealed in WHOIS?*
* *Should registrant be notified and how? Consider option to surrender domain rather than publication of contact data*
* *Consider protections in cases where publication of physical address could endanger someone’s safety*

1. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
2. 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)?