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

**{A few edits proposed by Kathy Kleiman**

**And lots of other people too!}**

**As of 31 January 2014**

**New Suggested Grouping of Questions:**

* **MAIN ISSUES**
* **REGISTRATION** of privacy/proxy services;
* **MAINTENANCE** of privacy/proxy services;
* **CONTACT** point provided by each privacy/proxy service;
* **RELAY** of complaints to the privacy/proxy customer; and
* **REVEAL** of privacy/proxy customers' identities.
* **PUBLICATION** of privacy/proxy customers’ identities.
* **TERMINATION** of privacy/proxy service and/or registration.

**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, notwithstanding access to data by legitimate requestors.*
* *Consider customer option for different methods and notification issues[[1]](#footnote-1) where applicable laws so permit.*
1. What types of services should be covered, and what 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 bound to the same standards as accredited service providers?

**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?
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?
* *?*
* *How would such checks be conducted and to what level (e.g., following the levels of validation and verification set out in the 2013 Registrar Accreditation Agreement or some other level)?*
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.
* *Use “domain name registrants using P/P services” rather than “customers”?*

*[NOTE: ICANN staff should provide updates on transfer, renewal, dispute and PEDNR policies]*

**III. REGISTRATION**

Threshold Question:

Currently, proxy/privacy services are available to companies, noncommercial organizations and individuals.  Should there be any change to this aspect of the current system in the new accreditation standards?[[2]](#footnote-2)

1. 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?
* *Define “commercial purpose” – must there be actual “trading”, or does it include any online business purpose (e.g. including for information or education)?*
* *Should there be a definition of what constitutes trading? Purpose? Level?*
* *Any difference between “personal” vs “noncommercial” e.g what about noncommercial organizations or noncommercial purposes such as political, hobby, religious or parental?*

*Include whether registration is for commercial purpose (not just the use of the domain name)*

* *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 enquiring into “use” 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?
* *What about non-profits and other noncommercial organizations that use a domain name for noncommercial purposes?*

**IV. 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”?*
* *Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant’s respective jurisdictions?*

**V. 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?
* *If so, should this apply to all formats, or just email communications?*
* *Plus publication of email address of the complainant?* **I think “REVEAL of email address” is what was intended here. [Rationale: we are in the Reveal section, and intent of question seems to be whether person providing allegation of illegal activities should be allowed to get the email of the p/p customer to directly send letters/demands/queries. It’s a good question. Note: Publication does not seem to be raised here at all.]**
* *Any difference if enquiry is from law enforcement, private attorney or other parties?*
* *Should the P&P Service refrain from forwarding the allegations to the customer if the enquire asks not to do it and reasons its request?*
* *Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant’s respective jurisdictions?*
* *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 or law enforcement request)?*

**VI. REVEAL**

1. What, if any, are the baseline minimum standardized reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
* *Any difference if requestor is law enforcement or a private party?*

*SUGGESTED ADDITIONAL SUB-QUESTIONS:*

* *What processes or levels of revealing the underlying registrant exist?*
* *What are the minimum standards of proof that should be required for the identity of the requestor?*
* *What are the minimum standards of proof that should be required for the allegations being raised by the requestor?*
* *Does the P&P service have to assess the lawfulness of the request?*
* *What limitations should the requestor be required to agree to regarding use of the revealed data (e.g., only for the purpose stated in the request and not for publication to the general public)?*
1. 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?
* *When should P/P providers be required to do this?*
* *Clarify that this relates to service of letters by private attorneys (and other parties?)*
* *Should notification of the customer also/ be required?*
* *When should customer be notified? Under what circumstances can customer contest the reveal before it takes place?*
* *Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant’s respective jurisdictions?*
1. What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger a reveal? What specific alleged violations, if any, would be sufficient to trigger a reveal ?
* *Not “publication” but disclosure by private parties*
* *Any difference if requestor is law enforcement vs. private party; if requestor is from different jurisdiction than P/P provider; or if laws are different in P/P provider and registrant’s respective jurisdictions?*
1. What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
* *Protections to cover both individuals and organizations*
* *Safeguards needed also for small businesses/entrepreneurs against anti-competitive activity, as well as for cases of physical/psychological danger (e.g. stalking/harassment) perhaps 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?*  **Huh? I don’t understand this bullet point. Revealed is to a Requestor; published is to the Whois database.**
* *Should registrant be notified prior to publication?*
* *Consider protections in cases where publication of physical address could endanger someone’s safety* ***–* Recommend expanding this bullet a little (per my original proposal) to include evaluation of organizational safety. E.g. expand to include: *Consider protections in cases where publication of a physical address could endanger the safety of an organization or association. Examples here include: churches, synagogues and mosques in minority areas and political and dissent groups and their locations.***
* *Is publication of the registrant’s contact data in WHOIS a threshold issue for this WG or should it be left to the respective policies of the P/P service provider (as agreed to by the registrant)?*
1. What safeguards or remedies should be available in cases where publication is found to have been unwarranted?
2. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
3. 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)?

**V!. PUBLICATION**

**V!!. TERMINATION**

* How will disputes about accreditation of a P/P service provider be resolved?
* What will be the process for complaints that a particular accredited provider no longer satisfies accreditation standards?
* Would there be an appeal mechanism if a provider is denied accreditation?

ADDITIONAL SUGGESTED GENERAL QUESTION:

* *Are there other issues we should be taking into account regarding Registrants [providers of the data], P/P service providers, and Requestors, both public and private [users of the data]?*
1. Several sub-questions seem to be conceived as though all P&P customers were in need of anonymity and were vulnerable and susceptible to harassment, political persecution or other evil consequences when evidence so far shows that P&P Services are greatly used to conceal people or organizations´ identities and contact data who are engaged in some sort of malicious or illegal activity.

 To erase the bias in the questions, they need to be reworded. I make some comments and suggest a different approach to them in each case.

 I copy below the last paragraphs of the NPL´s Study on Whois Proxy & Privacy Service Abuse, September 2013:

 “To summarise the whole project and to return at the end to our original hypotheses – we DID find clear evidence that:

 "A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity".

 But, although we did find that it was often true, we DID NOT find that in all cases:

 "The percentage of domain names used to conduct illegal or harmful Internet activities that are registered via privacy or proxy services is significantly greater than the percentage of domain names used for lawful Internet activities that employ privacy or proxy services."

 Additionally, we learnt that these statements ARE correct:

 "When domain names are registered with the intent of conducting illegal or harmful Internet activities then a range of different methods are used to avoid providing viable contact information – with a consistent outcome no matter which method is used.

 However, although many more domains registered for entirely lawful Internet activities have viable telephone contact information recorded within the Whois system, a great percentage of them do not." [↑](#footnote-ref-1)
2. Several WG members noted that some questions in this Section are somewhat conditional, in that a Yes/No answer to one may obviate the need to answer others. The “use” of a domain for specific purposes may also implicate content questions. The WG agreed that these issues should be flagged for discussion when considering the WG’s response to this Section. [↑](#footnote-ref-2)