PPSAI Work Plan Mind Map

Project Information

- Working Group Workspace: https://community.icann.org/x/9iCfAg
- WG Leadership: Don Blumenthal (Chair), Steve Metalitz (Vice-Chair), Graeme Bunton (Vice-Chair)
- WG Charter: https://community.icann.org/x/pCifAg

Basic Requirements

- Review of background documents (see https://community.icann.org/x/XSWfAg)
- Development of Work Plan
- (Working) Definitions of main terms
- Outreach at an early stage to other ICANN Supporting Organizations / Advisory Committees — Requests sent out (deadline for input 28 Feb)
- Request GNSO Stakeholder Groups and Constituencies for input — Requests sent out (deadline for input 28 Feb)
- EWG Survey
  - WG reviewed draft EWG questions and provided input on possible additional questions
  - Review survey results once available
- Survey of WG members may help to identify controversial / non-controversial topics — Survey launched (https://www.surveymonkey.com/s/86N33WX) - 6 responses received to date
- Staff to contact registrars under 2013 RAA with affiliated privacy/proxy services to obtain information on terms & conditions
- WG to review proposed categorization of charter questions and identify issues that need to be considered for each charter question

What additional information should be gathered / reviewed at the outset of the process? E.g. additional information on current practices? If so, also consider how this may link to the survey the EWG is planning '*on the existing practices of current providers of such services, with respect to their relay, reveal, and unmask procedures, and the conditions applicable to them. Also, the EWG is interested in the level of verification or validation conducted by such providers, if any, on the data provided by their customers*'.

Charter Questions

**What information is required in order to be able to answer these Charter questions?
Would it be helpful to group certain questions together in clusters?
What would be the most efficient way and/or order for the WG to tackle these questions?
Would it be helpful to conduct a survey amongst the WG members on each of these questions to get an idea where people stand (which may also help determine which are questions that might be easy to tackle and which one may be more complex)?**

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
4. *What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension of registrations?*
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?*
   - Postpone this discussion given that the RAA only went into effect on 1 Jan 2014?
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 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?*
   - What is the RAA's current requirement on this point?
   - How would such checks be conducted and to why level (e.g., following the levels of validation and verification set out in the 2013 RAA or some other level)?
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.*
   - Use "domain name registrants using P/P services: rather than "customers"?
   - NOTE: ICANN staff should provide updates on transfer, renewal and PEDNR policies

III. REGISTRATION

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?
2. *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 to 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?
3. *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 on to the customer all allegations they receive of illegal activities relating to specific domain names of the customer?*
   - Plus publication of email address?
   - Any difference if enquiry is from law enforcement, private attorney or other parties?
   - 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)?

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 private party?
   - What are the minimum standards of proof that should be required for the allegations being raised by the requestor?
   - What jurisdiction should govern whether allegedly problematic content is legal (e.g., comparative advertising is legal in the US, but not in Germany)?
   - 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)?
2. *Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for the specific purpose of enduring 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 request 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?
3. *What forms of alleged malicious conduct, if any, and what evidentiary standard would be sufficient to trigger such disclosure? What specific violations, if any, would be sufficient to trigger such publication?*
   - Not "publication" but disclosure by private parties
   - Any difference if request 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?
4. *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?
5. *What safeguards or remedies should there be for cases where publication is found to have been unwarranted?*
   - Not just published but revealed in Whois?
   - Should registrant be notified prior to publication? Will registrant have time to take action to protect home/business/noncommercial organization? 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
   - If 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)?
6. *What circumstances, if any, would warrant access to registrant data by law enforcement agencies?*
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)?*
   - 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]?