PPSAI Work Plan Mind Map

Project Information

- Working Group Workspace: https://community.icann.org/x/9iCfAg
- WG Leadership: TBC
- 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
- Request GNSO Stakeholder Groups and Constituencies for input
- Communicate information re. EWG Survey to WG
- Survey of WG members may help to identify controversial / non-controversial topics
- Consider survey / poll of Registrar WG members who may be able to provide information / insight into current practices
  - Consider breaking the survey / poll down across groups (e.g. registries, registrars)

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

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. What, if any, are the baseline minimum standardized relay and reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
3. Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for this specific purpose?
4. 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?
5. What forms of malicious conduct (if any) and what evidentiary standard would be sufficient to trigger such disclosure? What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
6. What specific violations, if any, would be sufficient to trigger such publication? What safeguards or remedies should there be for cases where publication is found to have been unwarranted?
7. Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
8. What are the contractual obligations (if any) that, if unfulfilled, would justify termination of customer access by ICANN-accredited privacy/proxy service providers?
9. 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.
10. 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?
11. Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
12. What measures should be taken to ensure contactability and responsiveness of the providers?
13. 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?
14. What are the forms of malicious conduct (if any) that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?
15. What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
16. 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)?
17. 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? Should there be a difference in the data fields to be displayed if the domain name is registered/ used for a commercial purpose or by a commercial entity instead of to a natural person?
18. Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?
19. What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension of registrations?
20. Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?

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)?