Proposed Grouping of Charter Questions – 23 December 2013

Covered services, eligible customers/users, and relations between them

- What types of services should be covered?

- Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?
    - *Yes. Privacy services should be a form of blocking data from the public view. They should require the data be verified prior to private registration. Privacy services should be offered for each data field individually. Without the public's ability to access the accuracy of registrant data, privacy providers must verify such data for operational accuracy. Privacy providers must also establish a clear ability to relay correspondence to the registrant, and the registrant must certify that they continue to receive these communications. Proxy services should constitute a legally binding agreement requiring the proxy provider to take on the responsibilities and liabilities of the registrant. Proxy providers may determine their own contracts with registrants with little to no ICANN oversight, but ultimately will be held responsible for any registrant misconduct.*
    - *I believe only ICANN accredited registrars should be privacy/proxy service providers, as under the registrar obligation for RDE can the correct information be provided to the data escrow service.*
    - *Yes. A proxy service is different in that it actually takes on the roll as Registered Name Holder, and that should be made very clear. Alternatively, perhaps only privacy services should be allowed.*

- Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?
    - *Yes*
    - *No*
    - *Yes, only natural persons for non-commercial purposes.*
    - *I refer to my answer above. Evildoers always look for holes in laws to take advantage of them*.

- 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?
    - *Yes. Commercial entities do not enjoy the same liberties of privacy that individuals have. Further, many countries mandate public commercial information, by way of consumer protections and anti-fraud laws. If a commercial entity is a registrant, no privacy or proxy services should be offered. If a domain name is being used for commercial purposes, an unmasking procedure should be triggered.*
    - *This would be a minefield to implement, and just would put more strain on the registrar.*
    - *P/p services should only be used by natural persons not involved in commercial activities. To the arguments that have been made for allowing commercial use, all I can say is that is what lawyers are for.*
    - *If a distinction is made, wrongdoers would automatically label their activities as personal. For instance, many IPR infringers are done by individuals. The answer to the second question is no. Should there be a difference in the data fields, they ought not prevent law enforcement authorities and courts of any jurisdiction from accessing all necessary data the service keeps.*

- 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 (Post Expiration Domain Name Recovery) policies should apply.
    - *Private individual registrants should have the right to protected information that will not be shared without substantial evidence of a breach of contract, including violations of applicable law. Privacy and proxy service providers should have clear policies for reveals, unmasking, transfers, and renewals. Two separate forms of transfers may occur. The first would be a transfer of the registrar which may or may not be the*

privacy/proxy service provider. The second would be the transfer of information from one privacy/proxy service provider to another. Both forms of transfer should occur without revealing registrant data. If a registrant has pending allegations or violations against them the domain and/or privacy/proxy service should not be transferable until the claims are resolved.

- *For any privacy protected domain, no transfer should be allowed whilst enabled as this hinders future ICANN processes if required, for example transfer disputes.*
- *For customers, the same as any Registered Name Holder. For p/p services, the same as any accredited registrar. All other policies should apply just as they do for any other registrant or registrar.*

- Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
    - *All privacy/proxy services should be required to verify operability of all contact information that they will be protecting, prior to beginning service. This can be accomplished the same way any other escrow service or online data protection firm does, via SMS, postal mail, robo-calls, and/or valid IDs. This information should be to some extent re-verified annually and all information should be re-verified over a period of three years.*
    - *No, the icann registrar is already achieving this.*
    - *Yes. Use the same processes and requirements of the new RAA.*
    - *Yes. It is likely that customers disguise their identity or provide false or inaccurate contact data if their data may be revealed to third parties entitled to have access to that information. See safeguard 1, annex I of GAC advice on new gTLDs (Beijing Communiqué)*

- What are the contractual obligations (if any) that, if unfulfilled, would justify termination of customer access by ICANN-accredited privacy/proxy service providers?
    - *Failure to acknowledge, through some form of an email receipt,*

correspondence sent through the privacy/proxy relay in a timely fashion should unmask the registrant's whois data. The registrant would not have to reply to the sender, but must click a link or respond to the provider to acknowledge the correspondence was received. Additionally, providers should be allowed to cease providing service to a registrant after providing timely notice to the contact information provided by the registrant. Lastly, providers should have the right to draft language into their contracts allowing for termination upon instances such as, illegal activity, failure to pay for services, or failure to comply with required provider communications.

- *Compliance with the registration agreement of the registrar of record, maintaining accurate contact info, and not engaging in commercial activities.*
- *Failure to provide real, useful and accurate identification and contact details.*

Standards Services Practices and Abuse/Misuse

- What, if any, are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?
    - *The Standard Service Practices should include: reveal procedures/criteria, unmasking procedures/criteria, legal relationships with ICANN and other ICANN contracted parties, quantitative metrics surrounding ICANN policy compliance, and what types of users or use are eligible for privacy and proxy services.*
    - *Such services should only be used by natural persons not involved in a commercial venture. Other practices should be developed by reviewing various Governmental privacy regimes, adopting rules/policies that are appropriate.*

- What, if any, are the baseline minimum standardized relay and reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
    - *Registrants should be required to respond to requests for information from the privacy/proxy provider in a timely manner. Failure to acknowledge correspondence should trigger an unmasking procedure. At*

any time, if a privacy/proxy provider is aware that the registrant is engaged in commercial activity in a way that is non-compliant with applicable law through use of the domain name, the provider should be permitted to reveal without recourse. Failure to reveal in light of a preponderance of evidence of commercial activity in violation of applicable laws should be arbitrated by the privacy/proxy provider accrediting body, and should be considered as cause for potential sanctions against the ICANN-accredited privacy/proxy service providers. As a fundamental principle, privacy/proxy providers should reveal registrant data if the registrant is using the domain name for commercial purposes.

- *Essentially a legal stance should be taken for removal of or providing of private information. The issue being as 1 example European Privacy law will ultimately get involved if the registrant is within europe.*
- *At a minimum reveal should occur upon being presented with a court order. Other policies for reveal should be adopted based on the privacy regime review mentioned in my response to 2. Relay should be as broad as is practical, only allowing non-relay based on "normal" procedures currently in use for filtering spam, junk mail, etc.*

- Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities? If so, under what circumstances? [This question seems duplicative of the preceding question?]
  - *Providers should be required to reveal customer identities if they are aware that: the domain name is clearly being used for commercial purposes, the registrant is identifying itself as a commercial entity by the content of the website, or if they are provided with a preponderance of evidence of illegal activity or contravening ICANN policy.*
  - *only if backed by LEA and/or court order*
  - *Yes.*

- 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?

- *No. Particularly when the allegation comes from a law enforcement agency, relaying that information to the registrant simply provides a likely criminal with notice that they are under investigation, and results in them taking immediate steps to further conceal their activities in other ways in order to stymie the investigative process. Conveying the information to the registrant in these cases would be a boon for cybercrime. Moreover, there is no parallel right in the "offline" world for the subject of an investigation to be notified once they are under investigation. Doing so would violate common sense. A clear boundary must be established between communications intended to be relayed to the registrant and the provider. The provider may not act as a mere go between, it must provide a service to both end users of the Internet and the registrant. If an allegation is directed to the registrant, the provider should relay the communication just like any other correspondence.*
- *Certainly, you are innocent until proven guilty.*
- *Yes.*
- *No. Whenever courts or competent public authorities request not to do so and justify the need not to frustrate an investigation, they shouldn´t do it.*

- What forms of malicious conduct, if any, and what evidentiary standard would be sufficient to trigger disclosure of registrant contact information to a complainant? What safeguards must be put in place to ensure adequate protections for due process, privacy, and freedom of expression?
    - *Any violation of applicable law should suffice to represent malicious content. The standard should be a preponderance of evidence. It is important to note that applicable law is not merely the jurisdiction of the registrant or the privacy/proxy provider, but also any jurisdiction in which the registrant is attempting to market goods or receive benefits from. In other words, even if it's legal to sell black tar heroin in the country in which the registrant and provider are located, it is still a violation of applicable law to advertise and facilitate the sale of black tar heroin to the US, and most other countries.*
    - *Again, routed through the LEA etc*

- *Again, there should be no more or no less protection than currently provided by existing privacy regimes for natural persons not involved in commercial activities.*
- *Asking for a court order in the jurisdiction of origin that would then need to be recognized and enforced in the jurisdiction of the privacy/proxy service provider or directly before the jurisdiction of the latter, where the reason and documentation of the disclosure request would not be warranted under the Universal Declaration of Human Rights, the International Covenants on Civil and Political Rights and on Economic, Social and Cultural Rights and other International Instruments on Human Rights adopted by the UN. This restriction should be applied only in unambiguous cases of threats to freedom of expression or other fundamental rights. Otherwise, data should be disclosed to national or foreign law enforcement authorities.*

- What specific violations, if any, would be sufficient to trigger publication [of registrant contact information by accredited providers]? What safeguards or remedies should there be for cases where publication is found to have been unwarranted?
    - *Any violation of applicable law should suffice to represent malicious content. In the instance of an unwarranted publication the registrant should have a private right of action against the alleging party, provided that the alleging party acted in bad faith. This can be handled via both contract law and applicable data protection laws. In all instances, the provider should be protected when they choose to reveal, unless the provider acted negligently or in bad faith.*
    - *You cannot be specific, its all based on a case by case basis*
    - *See 2 and 3 above. [Such services should only be used by natural persons not involved in a commercial venture. Other practices should be developed by reviewing various Governmental privacy regimes, adopting rules/policies that are appropriate. - At a minimum reveal should occur upon being presented with a court order. Other policies for reveal should be adopted based on the privacy regime review mentioned in my response to 2. Relay should be as broad as is practical, only allowing*

non-relay based on "normal" procedures currently in use for filtering spam, junk mail, etc.]

- What would be the forms of non-compliance that would trigger cancellation or suspension of registrations?
    - *Breach of the provider/registrant contract should trigger known and documented procedures for cancellation. The procedures should be clear in order to limit transfers and substantial changes to domain name contact information while the service is being suspended or cancelled. Allowing a registrant to modify all the verified contact information, providing inaccurate information, before a cancellation or suspension would undermine the initial verification of the registrant data.*
    - *Registration to a registrar means domain registration, it is not for the WG to be involved in the de-registration of a domain name.*
    - *Failure to provide correct identification data or, if the registrant sells the domain name to someone else, to identify the person responsible for the online content or activity located at the domain name.*

- What circumstances, if any, would warrant access to registrant data by law enforcement agencies?
    - *The standard must not require a court order. With the speed at which criminals may set up, move, redistribute and take down domain names, it is impossible for the world's judicial systems to keep pace. Moreover, the criminal activity may be targeting a jurisdiction other than that where the registrar is located, making a court order a practical impossibility in some cases. A preponderance of evidence of any violation of applicable law should suffice to represent malicious content.*
    - *Again case by case and dependent on what information is provided to privacy/proxy service.*
    - *See 2 and 3. [Such services should only be used by natural persons not involved in a commercial venture. Other practices should be developed by reviewing various Governmental privacy regimes, adopting rules/policies that are appropriate. - At a minimum reveal should occur upon being presented with a court order. Other policies for reveal should*

be adopted based on the privacy regime review mentioned in my response to 2. Relay should be as broad as is practical, only allowing non-relay based on "normal" procedures currently in use for filtering spam, junk mail, etc.]

- *In the above situations, where law enforcement authorities need to ascertain the identity and contact data of infringers.*

- 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 processes should focus on: clearly conveying who/what organizations or individuals may submit complaints (and if any organizations gain a "trusted" status); what type of information will be required for the service to consider that a preponderance of evidence has been established; and whether (and in what cases) an "appeal" will be provided to the registrant.*
    - *That's for the WG to consider*
    - *See 2 and 3. [Such services should only be used by natural persons not involved in a commercial venture. Other practices should be developed by reviewing various Governmental privacy regimes, adopting rules/policies that are appropriate. - At a minimum reveal should occur upon being presented with a court order. Other policies for reveal should be adopted based on the privacy regime review mentioned in my response to 2. Relay should be as broad as is practical, only allowing non-relay based on "normal" procedures currently in use for filtering spam, junk mail, etc.]*

Accredited Provider Requirements

- What measures should be taken to ensure that providers can be contacted that and that they are responsive to inquiries?
    - *Each form of contact that is relay-able to the registrant should be relayed in a timely manner. Clearly forwarding an email to a registrant can be automated and rapid, while postal mail may be more time consuming. Providers should also respond to reveal requests and*

allegations of criminal contact in a timely fashion. Reasonable time frames for both relays, and external requests should be mandated in the contract between ICANN and the providers.

- *Email should be more than sufficient, even within a ticket system for processing and completing any complaint.*
- *Periodic checks by ICANN Compliance, also following up on any related complaints.*
- *Banning them from holding more domain names, seizing revenues from "registrations", stripping them of their accreditation to be a proxy/privacy service and ordering the transfer to another service of the names they hold, imposing a hefty fine on them (a 20% of their income last year)...*

- 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?
  - *Yes, however 3.18.2 should be modified to include complaints from all applicable jurisdictions, not just the registrars.*
  - *Yes, simple email address for abuse.*
  - *Yes and Yes.*
  - *More or less. Section 3.18.1 should apply in its entirety. In Section 3.18.2 time requirements could be more flexible, but they should attend to requests by authorities anywhere, not only in the jurisdiction of their establishment. Section 3.18.3 should also be applied, but for services based in Europe, records would only be maintained for the time allowed by Data Protection legislation.*

- Shall designated published points of contact at an ICANN-accredited privacy/proxy service provider be responsible for addressing malicious conduct by registrants that use the provider's services? If so, what forms of conduct should be included?
  - *Any violation of applicable law should suffice to represent malicious content. It is important to realize applicable law is not merely the jurisdiction of the registrant or the privacy/proxy provider, but also any*

other jurisdiction in which the registrant is attempting to market goods or receive benefits from.

- *This question isn't very clear, but accredited p/p services should be required to have an agreement with their customers. It should require compliance with the Registration Agreement of the applicable registrar, which should already include standards conduct. If breached, the p/p provider should be required to cancel their service and notify the registrar of record, who may take the appropriate action regarding the domain name registration itself.*
- *It´s difficult to identify all possible sorts of misconduct. Refer to Safeguard 2 of annex I of GAC advice on new gTLDs.*

- 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?
  - *Yes. All non-ICANN accredited privacy/proxy service provider entries should be treated as Whois inaccuracies.*
  - *Yes*
  - *Yes.*
  - *Definitely yes.*

- Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?
  - *Yes. There also needs to be transparency and accountability as to the identities of accredited privacy/proxy service providers. Without full contact details it may become much more difficult to contact the provider, in order to submit abuse complaints to the service provider or relay any additional correspondence to the registrant.*
  - *Already within the 2013 raa*
  - *Yes.*
  - *To the same extent registries and registrars must provide them. But if a yes or no is needed, I would say yes.*