GNSO PRIVACY & PROXY SERVICES ACCREDITATION ISSUES (PPSAI) PDP WORKING GROUP

SUMMARY OF PRELIMINARY CONCLUSIONS[1] TO DATE ON CHARTER CATEGORIES A - E

Introduction

The PPSAI Working Group (WG) categorized the questions it was chartered to answer as follows:

A. **MAIN ISSUES**

B. **MAINTENANCE of privacy/proxy services**

C. **REGISTRATION of privacy/proxy services;**

D. **CONTACT point provided by each privacy/proxy service;**

E. **RELAY of complaints to the privacy/proxy customer;**

F. **REVEAL of privacy/proxy customers' identities; and**

G. **TERMINATION of [accreditation of][2] a privacy/proxy service**.

The chart below lists all the WG's Preliminary Conclusions on **Categories A through E** as of 3 October 2014.

CATEGORY A QUESTION 2: Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?
WG Preliminary Conclusion: Privacy and proxy services could potentially be treated the same way for the purpose of the accreditation process.

CATEGORY B QUESTION 1 - Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made

[1] These conclusions are considered preliminary as, following the WG's initial work on all the Charter questions, the WG will return to review each preliminary conclusion and, if necessary, update, add to or amend them.

[2] This term has been square bracketed in view of the WG call on 4 February. This issue is not specifically included in the WG Charter but the WG may consider it necessary or useful to provide general principles in the course of its deliberations that can guide the design and implementation of essential features of a de-accreditation/termination program. The Charter reflects community recommendations that were directed toward terminating customer access or registrar cancelation of registrations made by/via P&P services (see e.g. WHOIS RT Final Report, GNSO-ALAC RAA DT Final Report).

through a privacy/proxy service?

WG Preliminary Conclusion: Domain name registrations involving privacy/proxy service providers should be clearly labeled as such in Whois. There may be various ways to implement this recommendation in order to achieve this objective; the feasibility and effectiveness of these options should be further explored as part of the implementation process. As an example, it was suggested that P/P services could be required to provide the registration data in a uniform / standard format that would make it clear that the domain name registration involves a P/P service - e.g. entering in the field for registrant information 'Service Name, on behalf of customer' (in the case of a proxy service this could then include a number, customer #512, while in the case of a privacy service it would include the actual customer name). Following submission of this information to the registrar, this information would then be displayed in Whois making it clearly identifiable as a domain name registration involving a P/P service.

The WG also agreed there should be no distinction between privacy and proxy services for this purpose.

CATEGORY B QUESTION 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?

WG Preliminary Conclusion: The WG recommends[3] that proxy and privacy customer data be validated and verified in a manner consistent with the requirements outlined in the Whois Accuracy Specification of the 2013 RAA. Moreover, in the cases where validation and verification of the P/P customer data was carried out by the registrar, re-verification by the P/P service of the same, identical, information should not be required.

Similar to ICANN's Whois Data Reminder Policy, P/P providers should be required to inform the P/P customer annually of his/her requirement to provide accurate and up to date contact information to the P/P provider. If the P/P service has any information suggesting that the P/P customer information is incorrect (such as P/P service receiving a bounced email notification or non-delivery notification message in connection with compliance with data reminder notices or otherwise) for any P/P customer, the P/P provider must verify or re-verify, as applicable, the email address(es). If, within fifteen (15) calendar days after receiving any such information, P/P service does not receive an affirmative response from the P/P customer providing the required verification, the P/P service shall verify the applicable contact information manually.

[3] Some WG members are of the view that the minimum verification or validation standards for accredited services would need to exceed those applicable to non-proxy registrations, but this view could be affected by the outcome of discussions regarding relay and reveal requirements (e.g., re the speed of reveal). As such, this recommendation will be revisited upon the completion of the WG deliberations on the other charter questions.

CATEGORY B QUESTION 3 - What rights and responsibilities should domain name registrants that use 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?

WG Preliminary Conclusion: All rights, responsibilities and obligations for registrants as well as privacy/proxy providers would need to be clearly communicated in the privacy/proxy registration agreement, including any specific requirements applying to transfers and renewals (further details as to what minimum requirements for such rights, responsibilities and obligations to be discussed).

Specifically, in relation to transfers and renewals, the WG noted the common practice of terminating privacy/proxy protection as part of the transfer process and recommends that this be clearly disclosed to registrants (NOTE: a sub group was formed to explore practical ways to facilitate transfers without the need for termination).

The WG may explore the possibility of recommending that P/P providers report updates to Whois information within a certain time frame (e.g. modeled on Section 3.2.2 of the 2013 RAA).

The WG recommends that the following mandatory requirements form part of a P/P service accreditation program:

- All P/P services must relay to their customers any notices required under the RAA or an ICANN Consensus Policy.
- All P/P service registration agreements must state the customer's rights and responsibilities and the P/P service's obligations in managing those rights and responsibilities. Specifically, all P/P services must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name.

In addition, the WG recommends the following as best practices:

- P/P services should facilitate and not hinder the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the ERRP and transfers to another P/P service.
- P/P services should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name.

CATEGORY C[4]:
***"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[5]?*

The WG discussed the practical difficulties created by the lack of clear definition as to what is "commercial" and what is "noncommercial". For instance, a distinction could be made on the basis of the individual or organization having a certain corporate form, or on the basis of the activities/transactions the individual or organization engages in regardless of corporate form. In addition, some commercial entities register and use domain names for noncommercial (e.g. charitable or experimental) purposes.

The WG agrees that the status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether proxy/privacy services are available to the registrant. Fundamentally, p/p services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals.

However, a minority of WG members is of the view that domain names being actively used for commercial transactions (e.g., the sale or exchange of goods or services) should not be able to use or continue using proxy/privacy services. Accordingly, Charter Question C-1 presents some distinctions that create a division within the WG.

CATEGORY C QUESTION 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?

As noted above, the WG agrees that the mere fact of a domain being registered by a commercial entity, or by anyone conducting commercial activity in other spheres, should not prevent the use of p/p services. In addition, a majority of WG members did not think it either necessary or practical to prohibit domain names being actively used for commercial activity from using p/p services.

[4] The WG agreed to first discuss a Threshold (i.e. baseline) Question for this Category. In the course of deliberations it became clear that likely responses to Questions C-1 & C-2 were closely linked to this Threshold Question.

[5] In agreeing to first discuss this threshold question for Category C, WG members noted also that answers to some questions in this category might be somewhat conditional, in that a Yes/No answer to one may obviate the need to answer others. The WG also noted that references to the "use" of a domain for specific purposes may also implicate content questions.

However, a minority of WG members disagreed, noting that in the “offline world” businesses often are required to register with relevant authorities as well as disclose details about their identities and locations. These members expressed the view that it is both necessary and practical to distinguish between domains used for a commercial purpose (irrespective of whether the registrant is actually registered as a commercial entity anywhere) and those domains (which may be operated by commercial entity) that are used for a noncommercial purpose. However, domains that conduct financial transactions online must have openly available domain registration information for purposes of, for example, consumer self protection and law enforcement purposes. Accordingly, these members suggested that domains used for online financial transactions with a commercial purpose should be ineligible for privacy and proxy registrations.

Among the arguments in response, some WG members assert that in jurisdictions where similar legal requirements (e.g. business registration, disclosure of location) already exist for the "online world", such disclosures are generally made via a prominent link on the web site rather than in the WHOIS data. This is due apparently to the fact that, in the translation from the "offline world" to the "online world", legislators usually focus on the content available under the domain name, not the domain name registration itself. The majority view also holds that there may be valid reasons why domain name registrants using their domain names for commercial purposes may legitimately need the availability of such services (for example, for the exercise of political speech).

Question C-1 subparts (a) and (b), which the WG added early in our work to focus discussions, suggest defining “commercial” within the context of specific activities, and uses “trading” as an example. However, the WG discussion has focused on a broad term “commercial” and whether certain types of commercial activity mean that a domain is not eligible for P/P registration. For clarity as the WG moves forward, we will continue to use “commercial” in a broad sense and “transactional” to address issues raised by the position held by the minority group on the threshold question. The WG will develop a formal definition of “transactional” as needed for further discussion of the minority group’s approach.

CATEGORY C QUESTION 2 - Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

Given the foregoing discussion, the WG does not believe that privacy/proxy registrations should be limited to private individuals who use their domains for non-commercial purposes.

Issues discussed likely will arise with respect to matters that the WG will address later. In addition, the WG may consider requesting community feedback on this question as it continues its deliberations on the questions contained in its charter. The WG did note that per its preliminary agreement on question B-1 that 'domain name registrations involving privacy/proxy service providers should be clearly labeled as such in Whois. The WG observes that there may be various ways to implement this recommendation in order to achieve this objective and suggests that the feasibility and effectiveness of these options is further explored as part of the implementation process. As an example, it was suggested that P/P services could be required to provide the registration data in a uniform / standard format that would make it clear that the domain name registration involves a P/P service such as entering in the field for registrant information 'Service Name, on behalf of customer' (in the case of a proxy service this could then include a number, customer #512, while in the case of a privacy service it would include the actual customer name). Following submission of this information to the registrar, this information would then be displayed in Whois making it clearly identifiable as a domain name registration involving a P/P service'.

CATEGORY C QUESTION 3 - 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?

<u>WG Preliminary Conclusion</u>: A majority of WG members are of the view that it is neither desirable nor feasible to make a distinction in the data fields to be displayed.

CATEGORY D QUESTION 1- What measures should be taken to ensure contactability and responsiveness of the providers?

<u>WG Preliminary Conclusion</u>: ICANN should publish and maintain a publicly accessible list of all accredited p/p providers, with all appropriate contact information. Registrars should provide a web link to p/p services run by them or their Affiliates, and p/p providers should declare their Affiliation with a Registrar (if any) as a requirement of the accreditation program. The WG noted that responsiveness is a separate and necessary part of the accreditation program, but has not finalized agreement on the appropriate form and level of responsiveness to be required of accredited p/p providers.

CATEGORY D – QUESTION 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?

<u>WG Preliminary Conclusion</u>: The WG agreed that a "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes, noting that the primary concern is to have one contact point that third parties can go to and expect a response from. In this regard, the WG noted that the TEAC language of "capable and

authorized" could be helpful as a possible standard for a designated contact.

On responsiveness, the WG agreed to further discuss the sufficiency of a "reasonable and prompt" standard (per Section 3.18 of the 2013 RAA) under the Relay and Reveal categories.

The WG noted with approval the following recommendations from ICANN's Compliance Department (whose input the WG had sought in relation to the practical workings of Section 3.18 to date), and agreed they may be helpful in its further review of this question: (i) provide guidance to an abuse report requirement as to the types of abuse complaints allowed and types of actions P/P providers should take about these reports; and (ii) consider alternative abuse report options other than publishing an email address on a website and in Whois output (to address increasing volumes of spam).

CATEGORY D QUESTION 3 - Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required?

WG Preliminary Conclusion: The WG agreed that P/P providers should be fully contactable; it has yet to reach agreement on whether adopting Section 2.3 (from the 2013 RAA Temp Spec) will be sufficient, noting that this WG is making other recommendations in response to Charter questions that may affect the matter (e.g. the WG recommendation for ICANN to publish a publicly-accessible list of accredited providers (see WG Preliminary Conclusion for D-1), and for Whois entries to be clearly labeled if they are those of a P/P provider (see WG Preliminary Conclusion for B-1).)

CATEGORY D QUESTION 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?

WG Preliminary Conclusion: The WG recommends that the requirements in relation to which forms of alleged malicious conduct would be covered by the designated published point of contact at an ICANN-accredited privacy/proxy service provider include a list of forms of malicious conduct to be covered. These requirements should allow for enough flexibility to accommodate new types of malicious conduct. Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement[6] or

[6] "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."

Safeguard 2, Annex 1 of the GAC's Beijing Communique[7] could serve as examples for how this could be achieved.

Furthermore, the WG recommends a standardized form for information requests and reports, which would also include space for free form text. At a minimum such a form should include the following elements: *[to be completed]*. It was also suggested that providers have the ability to "categorize" reports received, in order to facilitate responsiveness.

CATEGORY D QUESTION 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?

WG Preliminary Conclusion: The WG recommends that the requirements in relation to which forms of alleged malicious conduct would be covered by the designated published point of contact at an ICANN-accredited privacy/proxy service provider include a list of forms of malicious conduct to be covered. These requirements should allow for enough flexibility to accommodate new types of malicious conduct. Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement[8] or Safeguard 2, Annex 1 of the GAC's Beijing Communique[9] could serve as examples for how this could be achieved.

Furthermore, the WG recommends a standardized form for information requests and reports, which would also include space for free form text. At a minimum such a form should include the following elements: *[to be completed]*. It was also suggested that providers have the ability to "categorize" reports received, in order to facilitate responsiveness.

CATEGORY E QUESTIONS 1 & 2 - What, if any, are the baseline minimum standardized

[7] "Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law."

[8] "Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."

[9] "Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law."

relay processes that should be adopted by ICANN-accredited privacy/proxy service providers? 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?

<u>WG Preliminary Conclusions on Electronic Communications:</u>

(1) All communications required by the RAA and ICANN Consensus Policies must be forwarded;
(2) For all other electronic communications, providers may elect one of the following options:

- <u>Option #1</u>: Forward all electronic requests received (including emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications
- <u>Option #2</u>: Forward all electronic requests (including those received via emails and web forms) received from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activity); and

(3) In all cases, providers must publish and maintain a mechanism (e.g. designated email point of contact) for requestors to contact to follow up on or escalate their original requests.

The WG also recommends that standard forms and other mechanisms that would facilitate the prompt and accurate identification of a relay request be developed for the use of accredited providers (e.g. drop-down menus in a provider's web-based forms or fields that would require the filling in of a requestor's contact details, specifying the type of request or other basic information).

Open Questions:

- Should providers be required to forward hard copy notices to registrants/customers, on request, in cases where electronic communications are known to be undeliverable?

- Should providers be permitted to charge a reasonable fee to forward non-electronic communications that incur a cost to do so (this could include monetary costs such as charges for registered mail and/or other resource costs such as man-hours to review/strip out personal information from a communication)?

- If a provider chooses not to forward an allegation of illegal activity, should there be an obligation for a provider to inform a requestor when the provider does not forward its request?