VIRTUALAW LLC

Philip S. Corwin, Founding Principal
1155 F Street, NW Suite 1050
Washington, DC 20004
202-559-8597/Direct
202-559-8750/Fax
202-255-6172/Cell
psc@vlaw-dc.com

July 7, 2015

By E-Mail to:comments-ppsai-initial-05may15@icann.org

Internet Corporation for Assigned Names and Numbers

12025 Waterfront Drive, Suite 300

Los Angeles, CA 90094-2536

Re: GNSO Privacy & Proxy Services Accreditation Issues Working Group Initial Report

Dear ICANN:

I am writing on behalf of the members of the Internet Commerce Association (ICA). ICA is a not-for-profit trade association representing the domain name industry, including domain registrants, domain marketplaces, and direct search providers. Its membership is composed of domain name registrants who invest in domain names (DNs) and develop the associated websites, as well as the companies that serve them. Professional domain name registrants are a major source of the fees that support registrars, registries, and ICANN itself. ICA members own and operate approximately ten percent of all existing Internet domains on behalf of their own domain portfolios as well as those of thousands of customers.

This letter addresses the GNSO Privacy & Proxy Services Accreditation Issues Working Group (WG) Initial Report that was published for public comment on May 5, 2015. I have participated in the deliberations of the WG as a representative of ICANN's Business Constituency (BC) -- but the views expressed in this letter are solely those of the ICA.

Summary of Position

ICA commends the effort of the WG's members to establish accreditation standards based on minimum baselines of conduct for privacy and proxy (P/P) services offered by ICANN-accredited registrars. We agree that final consensus recommendations, if approved by the GNSO Council and the ICANN Board, "will substantially improve the current environment, where there is presently no accreditation scheme for privacy and proxy services and no community-developed or accepted set of baseline or best practices for such services".

At the same time, the use of P/P services can be legitimate and necessary for both commercial and non-commercial domain registrants, and their privacy rights and expectations must be recognized and respected. The use of P/P services must be differentiated from the intentional furnishing of inaccurate WHOIS information, which we wholeheartedly deplore.

ICA's Code of Conduct long ago established this WHOIS standard for our members:

> *A registrant will provide accurate domain name ownership and contact information to the WHOIS database in a timely manner so that domain name ownership is transparent. While a registrant may use a proxy service or other accepted means of privacy protection, a registrant should provide a timely response to any inquiry passed on via such proxy or related service or received directly when such service has complied with a lawful request for contact information.*

Further, any policy development in this area must also recognize that P/P services are offered by other parties who are not under contract with ICANN – by law firms for their clients in particular -- and therefore are not subject to this policy development process and any resulting baseline requirements. Overreach in this area could have the effect of making fully reliable P/P services available only to well-heeled businesses and individuals able to afford access to legal services, while making lower-cost P/P services from registrars less effective as a privacy shield. Inordinate compliance demands on registrars could also have the effect of making P/P services substantially more expensive for those choosing to utilize those services offered by registrars.

In this comment letter we:

- Support adoption of the WG's Agreed Preliminary Conclusions
- Provide input on topics on which the WG has not yet finalized Preliminary Conclusions

- Oppose the general position that domain names that are actively used for commercial transactions should be prohibited from using P/P services, and offer further thoughts on this topic.
- **Express strong opposition to the information revelation framework proposed in Annex E of the Report, and express the contrary view that registrant data should only be revealed by the P/P provider in instances of a court order or a subpoena (in a competent jurisdiction to the P/P provider); a pending civil action; or a URS or UDRP action.**

Agreed Preliminary Conclusions

ICA generally supports all of the consensus recommendations contained in Section 1.3.1 of the Report. These consensus recommendations include definitions of key terms; WHOIS labeling requirements; validation and verification standards for customer data; mandatory provisions in provider terms of service; minimum requirements to be communicated to customers; recommended best practices; contactability and responsiveness standards for P/P providers; a standard form and requirements for abuse reporting and information requests; standards for relaying of third party requests; and standards for deaccreditation and its resulting consequences. Collectively, adoption of these consensus recommendations will go a long way toward establishing minimum guidelines and consistent practices among registrar-provided P/P services.

In particular, we support the position that:

> *The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether P/P 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. Further, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes.*

While we support the WG's position that *"none of its recommendations should be read as being intended to alter (or mandate the alteration of) the prevailing practice among P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a P/P service customer"*, we do have very strong concerns about the *"illustrative draft Disclosure Framework that would apply to Disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners"*. That Framework is provided in Annex E of the Report and, noting the statement that the Annex includes *"certain alternative formulations for which the WG has yet to*

***reach consensus and welcomes community input on"*, we provide additional input on it below.**

Topics on Which the WG has yet to Finalize its Preliminary Conclusions

ICA holds the following views on select topics in this category:

- Escalation of Relay Requests – We have no objection to requiring a P/P provider to forward upon request a further form of notice to its customer when there is persistent delivery failure of an electronic communication. However, we oppose the imposition of any fee on the registrant customer for doing so, or on the requesting party; the cost of such rare instances of additional outreach should be reflected in the annual cost of the P/P service.
- **Disclosure and Publication in relation to Requests by LEA and other Third Parties other than Trademark and Copyright Owners – We have not reached conclusions on the questions posed in this section – other than being in opposition to any mandatory compliance by P/P providers to requests for revelation of registrant data made by third parties other than law enforcement and IP owners outside the context of a court order or subpoena, a civil lawsuit, or a UDRP or URS action (our views on this topic are further discussed under the Annex E heading).**

Topics on Which There is Currently no Consensus Within the WG

ICA holds the following views on select topics in this category:

- **We oppose the general position that domain names that are actively used for commercial transactions (e.g. the sale or exchange of goods or services) should be prohibited from using P/P services.**

  Additionally, we oppose any suggestion that a domain employed in a "commercial use' should be barred from being under P/P protection. Our members have legitimate reasons for utilizing these services. For example, a valuable generic domain may be placed under P/P protection to assure equality of negotiating position if an offer is made to purchase it, as domain brokers will often shield the identity of a prospective purchaser. Or a domain may be leased for use by a third party and the domain owner may wish to shield its identity to avoid confusion regarding the identity of the owner and the licensee.

However, there may be a credible case for prohibiting the use of P/P services by websites that are actively and directly engaged in the provision of goods and services related to highly regulated industries such as banking, securities, insurance, and certain aspects of health care, and we would therefore not oppose further exploration of that subset of commercial activities as the WG continues its efforts. In regard to the proposition that *"domains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations"*, we could not support it unless it was severely limited in application to such services as online banking, and clearly excluded general financial transactions (e.g., acceptance of credit card payments at a website) as well as ad link-populated or general information websites relating to any commercial activity.

Accreditation Model

We have no particular views at this time on a proper accreditation model for P/P service providers other than that it should be integrated to the greatest extent feasible with the existing RAA so as to minimize accreditation and compliance costs.

Annex E Issues

The following statement is found at page 41 of the report:

> *The WG also acknowledged that there are various different grounds upon which third parties may request disclosure. These can include the initiation of proceedings under the UDRP,* ***allegations of copyright, trademark or other intellectual property infringement****, problems with the content of a website(s), and the distribution of malware. In addition, there are also different types of Requesters – such as LEA,* ***intellectual property rights owners or their attorneys****, and anti-spam and anti-phishing groups (among others). The WG noted that different standards and recommendations may have to be developed for either each type of request, or each type of Requester, or both.* ***At the moment, the WG has developed an illustrative Disclosure framework for requests made by trademark and copyright owners or their authorized representatives (see Annex E)****, and welcomes community input on the need for, and possible elements of, a similar framework for LEA and other types of third party Requesters.*

Annex E – the "Illustrative Draft Disclosure Framework for Intellectual Property Rights-holders" – appears at pp. 84 – 92 of the Report.

As a general matter we are strongly opposed to the revelation of a registrant's personal contact and other information hidden by their use of a P/P service to any third party other than a law enforcement agency (LEA) or other party that has obtained requisite approval from a court of competent jurisdiction, as reflected in a court order or subpoena.

We believe that absent a registrant's breach of material service terms such as Internet abuse, the only basis for a P/P service being compelled to disclose underlying Registrant data should be:

- **a court order (in a competent jurisdiction to the Proxy provider)**
- **a subpoena (in a competent jurisdiction to the Proxy provider)**
- **a pending civil action**
- **a URS or UDRP action.**

In all of these instances the registrant's personal information held by the P/P provider should not be revealed other than under seal to either the UDRP/URS provider or the court, with the opposing attorney informed that the information is under seal and for the attorney's eyes only. This is how all other personal information that is sensitive is handled in U.S. federal court and we believe it is the proper standard to use in these cases.

Therefore, we specifically oppose those provisions of Annex E that would authorize release of registrant information in instances where a domain name allegedly infringes a trademark. ICANN has provide two dispute resolution procedures for use by trademark owners in such instances, the UDRP (for all gTLDs) and the URS (for new gTLDs), and disclosure of registrant data to the complainant is provided for in those procedures. Mandatory revelation of registrant data by a registrar P/P where there is an allegation of an infringing domain name should be impermissible outside the UDRP and URS context.

Further, the standard proposed for revelation in Annex E for such cases – a "good faith statement that provides a basis for reasonably believing that the use of the trademark in the domain name allegedly infringes the trademark holder's rights and is not defensible" -- is significantly inferior to the "bad faith registration and use" standard for prevailing in a UDRP or URS. In addition, such requests could be filed by "authorized representative of the trademark holder" who are not attorneys and therefore not experts in trademark law, and not held to legal practice ethical requirements and potential sanctions for misuse of process or data.

While the proposed policy would *require "that Requester will use Customer's contact details only --*

i. to determine whether further action is warranted to resolve the issue;

ii. to attempt to contact Customer regarding the issue; and/or

iii. in a legal proceeding concerning the issue."

-- it is the unfortunate experience of our members that many trademark owners in possession of such information will utilize it to threaten and attempt to harass a registrant into surrendering their domain; or will utilize it in an attempt to "entrap" the registrant by making an offer to purchase the domain at an inflated price which, if accepted, will be rescinded and then cited as purported evidence of bad faith use in a subsequently filed UDRP for the purpose of reverse domain hijacking.

In regard to situation where a domain name resolves to website where trademark is allegedly infringed, we also oppose the proposed provisions of Annex E. While we recognize the existence of websites dealing in counterfeit goods and the significant harms that such activities may pose to the public, such actions could again be initiated by *"authorized representatives of the trademark holder"* who are not attorneys. This provision would also foist complex legal interpretative duties upon the registrar P/P provider, such as determining whether the registrant has *"a reasonable defense for its use of the trademark…content in question"*, which it is completely unqualified to determine and which can only be made by a court of competent jurisdiction or an impartial third party legal expert.

Likewise, the proviso that the P/P provider can refuse disclosure of registrant data where *"the Customer has objected to the disclosure and has provided [[adequate] [sufficient][compelling] reasons against disclosure, including without limitation a reasonable defense for its use of the trademark or copyrighted content in question] [a reasonable basis for believing (i) that it is not infringing the Requester's claimed intellectual property rights, and/or (ii) that its use of the claimed intellectual property is defensible]"* would again place the registrar P/P provider in the untenable and unsuitable position of acting as a court or expert arbitrator in regard to legal matters in which it has no competence or authority.

Thus, in regard to websites that allegedly deal in infringing goods and services, we oppose any proposal that would require the P/P provider to judge the sufficiency of the requester's allegations or the registrant's defenses. However, we also recognize that a trademark owner may be hindered in its ability to seek law enforcement assistance or determine the proper venue for a judicial action if it is unable to determine the identity

and locale of the domain registrant. Therefore, we would not object to exploration of the development of a rapid, impartial and expert dispute resolution process to consider requests for registrant data in regard to websites where trademark is allegedly infringed. This position is consistent with our view that registrant data can properly be revealed when a UDRP or URS is filed provided that proper protections accompany such disclosure.

As regards subsection D of Section III of Annex E, it proposes a policy that is exactly backwards. It currently reads:

> ***D. Disclosure cannot be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name.***

Most of Annex E should be scrapped and replaced by the simple principle that "Disclosure cannot be refused where the requester is acting pursuant to", with that introductory statement followed by the four instances cited above -- and with the further proviso that such disclosure shall be made under seal and provided solely to attorneys.

Finally, in regard to the proposal that, *"In the event that a Provider is alleged to have made a wrongful disclosure based on a Requester having provided false information, the Provider and Requester shall participate in an ICANN approved dispute resolution process",* the proposed arbitration procedure response is shockingly inadequate and far too limited to provide any appropriate redress for the disclosure of registrant personal data in response to requests knowingly made on the basis of falsified information. Only courts of competent jurisdiction can provide the necessary safeguards against such deliberate abuse and the stringent remedies to punish them.

Conclusion

We appreciate the opportunity to provide these comments on the GNSO Privacy & Proxy Services Accreditation Issues Working Group Initial Report. We hope that the WG finds them useful as it continues to strive toward development of a Final Report.

Sincerely,

Philip S. Corwin

Counsel, Internet Commerce Association