ANNEX A.

GAC PUBLIC SAFETY WORKING GROUP COMMENTS TO PROXY PRIVACY ACCREDITATION ISSUES

GAC Public Safety Working Group (PSWG) Comments to Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process[1]

After review of the Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process, the PSWG provides the following comments and recommendations:

Distinction between Commercial and Non---Commercial Users:

- In order to promote transparency and consumer safety and trust, the PSWG recommends against permitting websites actively engaged in commercial transactions – meaning the collection of money for a good or service – to hide their identities using Privacy/Proxy (P/P) Services.[2] This includes domains used for websites that directly collect payment data, as well as for sites that promote a transaction but directly link to other sites that execute the transaction. The public is entitled to know the true identity of those with whom they are doing business. Indeed, many nations have laws specifically mandating such transparency in commercial and business transactions.

- P/P services should only be permitted for those domains that are not actively conducting business transactions, as detailed in the above. Any person or entity that engages in commercial transactions invites the public to trust them with their funds and sensitive financial account information. Hence, any privacy interest should be balanced with the public's right to know the true identity of those with whom they are doing business.

Transparency and Accountability:

- The PSWG supports the conclusion that ICANN should ensure transparency by publishing and maintaining a publicly accessible list of all accredited P/P service 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 service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program.

[1] These comments were produced by an internal GAC Working Group and do not represent a consensus GAC view.

[2] Any definition of "commercial transactions" and limitations on use of P/P services should not apply to registrants whose sites are supported by advertising (and thus arguably "commercial"), but are not actively engaged in financial transactions.

GAC PUBLIC SAFETY WORKING GROUP COMMENTS TO PROXY PRIVACY ACCREDITATION ISSUES

- The PSWG supports the conclusion that a "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes and a designated point of contact should be "capable and authorized" to investigate and handle abuse reports, consistent with RAA Section 3.18.
- The PSWG agrees that proxy and privacy services should be treated equally for the purpose of accreditation process.
- The PSWG concurs with the P/P WG preliminary conclusion that domain name registration involving P/P service providers should be clearly labelled as such in the WHOIS.

- The PSWG recommends that P/P customer data should be validated in compliance with the RAA Cross---Validation requirement, pursuant to RAA WHOIS ACCURACY PROGRAM SPECIFICATION, paragraph 1 "… Registrar will, with respect to both WHOIS information and the corresponding customer account holder contact information related to such Registered Name…" validate the information provided.

- PSWG believes that proxy/privacy services should continue to be required to publish their relevant terms of service and to abide by those published terms (as currently provided in the Interim Specification to the 2013 RAA).

<u>Definition of Law Enforcement</u>

- "Law Enforcement Authority" is defined as "law enforcement, consumer protection, quasi---governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the privacy or proxy service provider is established or maintains a physical office." To the extent this definition could be viewed as suggesting that P/P service providers need only respond to law enforcement authorities within their own jurisdiction, the PSWG urges the P/P Working Group to consider revising this definition. Malicious conduct involving domains often takes place across borders and the definition of law enforcement should recognize the multi---jurisdictional aspects of investigative and enforcement activities in order to promote protecting the public no matter where they are located. If such revisions are made, the Working Group should consider a requirement that a P/P service consult with its local law enforcement authorities in the event it receives a request from a foreign authority (to ensure that the local authorities believe that the request is a proper request from a recognized foreign authority).

GAC PUBLIC SAFETY WORKING GROUP COMMENTS TO PROXY PRIVACY ACCREDITATION ISSUES

Confidentiality of Law Enforcement (including Consumer Protection) Requests

- Although the Initial Report did not reflect an agreement on the issue of whether P/P Service Providers should disclose requests from law enforcement, the PSWG appreciates the Initial Report's recognition of the "need for confidentiality in relation to an ongoing LEA investigation." Section 1.3.2 at p. 15. Law Enforcement Agency and Consumer Protection Agency (collectively "LEA") requests are directly related to ongoing investigations. Notifications to customers, who may be the alleged criminal or violator, could threaten not only the effectiveness of the investigation but could also threaten the safety of individuals. Accordingly, the PSWG urges P/P Working Group to require P/P Service Providers to keep LEA requests confidential as required and/or permitted by local laws.
- Requests by LEAs are directly related to sensitive investigations involving violations of the law. Many malware and other seemingly less critical violations have hidden connections to more malevolent criminal enterprises. Given the variety of subject areas for LEA investigations, it would be virtually impossible to confine the topics of potential investigations into select categories for the purposes of P/P Services. If a P/P provider were to provide notice of a LEA investigative request to the target of the request, remedies for such disclosure by the P/P provider would be determined by the respective national, state, provincial, or other governing laws.
- The confidentiality of individual requests does not impair the P/P service providers in publishing statistics in the form of transparency reports on the law enforcement requests received.

Conclusion

Public safety authorities, including law enforcement and consumer protection agencies, play a vital role in responding to incidents of crime, victim distress, potential harm, and in worst case scenarios, victim identification. To the extent, privacy services are used to hide the actors responsible for malicious activities or obscure other pertinent information, there must be reasonable mechanisms in place for public safety authorities to unmask bad actors and obtain necessary information. We urge the P/P Working Group to take into account the law enforcement need to obtain information cloaked by privacy services in order to continue to protect the public from malicious conduct that involves internet domains.