

ALAC Statement on the GNSO Privacy & Proxy Services Accreditation Issues Working Group Initial Report

The ALAC welcomes the opportunity to respond to the Initial Report of the Privacy and Proxy Services Accreditation Issues Report.

The ALAC's response is grounded on four general principles we believe must drive development of the Specifications:

- The protections provided in the final Specification should not be less than that which is required under the Interim Specification There is no discrimination for accessing privacy and proxy services by either natural or legal persons provided the rules developed apply equally across all classes.
- A balance must be struck between legitimate privacy rights of individuals and the legitimate needs of law enforcement and others in determining when and in what circumstances a privacy or proxy service customer's personal information will be revealed or published. Such balance must clearly embrace the rights of individuals to seek redress,
- The specifications may not be so onerous as to result in a chilling effect for users to access privacy and proxy services.

The ALAC's responses to specific questions raised in the Issues Report are as follows:

When must contact requests to the customer be forwarded to the P/P customer?

We agree that all contact requests must be forwarded including:

- Those required under the RAA, and from ICANN;
- All requests from law enforcement agencies and other third parties alleging domain name abuse.

We hold that requests from law enforcement agencies and 'other third parties alleging domain name abuse' should include government agencies (in the jurisdiction of the p/p provider) charged with the regulation of potentially criminal behaviour such as fraud and/or consumer deprecations such as misleading and deceptive conduct in that jurisdiction.

It should be left up to individual p/p providers as to whether other contact requests are forwarded (possibly excepting spam, etc.). We recommend that the classes of such contacts subject be clearly stated and published in the provider's terms of service.

Should or must the provider forward a further request(s), at whose costs and should there be a limit on the number of requests?

In every day life, individuals are not required to respond to any communication, whether by post, telephone or other electronic communication. Communication through the Internet should not be treated differently.

In response to this question, it should be left up to the individual provider as to the circumstances in which a contact request will be forwarded by other means. Equally, it should be left to the provider as to

whether they are prepared to use other means to contact the customer and whether they are prepared to absorb the costs. In general terms, however, the cost should be on the party making a contact request.

In any event, persistent failure to reach a customer by means properly noted in the terms of service should trigger re-verification of customer's contact by the provider in keeping with existing terms of the RAA.

If the matter involves potentially serious criminal behaviour or serious misuse of the DNS, law enforcement agencies can become involved. In other cases, dispute resolution processes such as the UDRP can be used.

Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer?

Yes.

Should there be mandatory publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity?

Yes, when misuse of the DNS under the terms of the service and illegal activity is established. P/P Provider actions do not preclude other likely and more severe responses allowed by the RAA or in law.

Other questions raised in an Annex to the report include the following:

What (if any) should the remedies be for unwarranted Publication?

Once personal details have been made known either to an individual requestor or more broadly published, the damage has been done. Depending on the facts of each case, there may be compensation for damage caused by a breach of contract thru civil means. ICANN Compliance must be notified since such breach may also amount to a breach of the Specification.

Should requestors be allowed to escalate every request to a 3rd party forum or should the WG develop standards and thresholds?

Again, it should be up to individual providers on how they handle contact requests from third parties, as long as the customer is informed of the individual provider's policies on this issue.

Should registrants of domain names associated with commercial activities and which are used for commercial online financial transactions be prohibited from using, or continuing to use, p/p services?

No. Commercial online financial transactions can be provided by a range of people/organisations including charities, human rights organisations, women's refuges or other entities that may have quite legitimate reasons for the use of p/p services but want to engage in fund raising activities. Trying to draw a distinction between charitable, human rights or other fund raising activities and other

commercial online transactions would be extremely difficult for p/p providers that would have to decide whether to allow such an entity to use a p/p service - in advance of allowing the entity to subscribe to the service.

If the commercial entity does misuse the service, we are recommending that not only law enforcement agencies, but also other government agencies charged with corporate and consumer protection be given access to relevant Whois data.

Finally, one issue that was not addressed in the Issues Report, but is of concern to the ALAC is compliance with the Specification. Under the 2013 RAA, registrar compliance with the Specification is required, and through the Registrar, its affiliates and resellers.

Proxy services can be provided by a registrant who, in turn, licenses the use of the domain name to their customer and it is the registrant's details that appear in the Whois database rather than the proxy service customer. In those circumstances, it may be possible for registrars (and their affiliates and resellers) to include in contracts with their customers (registrants), a requirement that if the registrant provides a proxy service, they will comply with the Specification. In that way, enforcement of specification requirements can be through that contractual arrangement.