Tiered Access Related Recommendations of GNSO Whois Task Force 1 and 2

Compiled by ross@tucows.com

June 28, 2005

This document outlines the recommendations of GNSO Task Force 1 and 2 relevant to the notion of implementing tiered access to gTLD Whois services. This is not an official document of the GNSO and should only be used for reference purposes.

Table of Contents

Whois TF1 – Tiered Access related recommendations

5. Changes should apply to all forms of access

To the extent that we are recommending any changes to access of Whois information, such changes need to be applied to all forms of access to Whois, whether Web-based, Port 43-based, or through any other mechanism.

6. Future of Port 43 Access
Based on input from the community, TF 1 has come to the conclusion that it is not possible to create technical restrictions under the current Port-43 specifications, that will limit port 43 access to a specific type of purpose; e.g., "nonmarketing uses." We have concluded that any access restrictions imposed on Port 43 by TF1 will apply to any Whois user, regardless of their purpose. In order to prevent abusive data mining by some on Port 43, we are required to develop access restrictions on Port 43 that affect all users and all purposes.

1. Currently, Port 43 does not provide a way for a requestor to identify him or herself or the reasons for which it is seeking the data.
2. If only Non-sensitive Data is displayed, there is little reason to change anything with respect to Port 43 .
3. If Sensitive Data will be displayed, then Port 43 would not be able to provide the functionality described in Section 4 above.
4. Port 43 should, however, not be shut down completely. The Task Force believes that unless other mechanisms were available to the Registrars to retrieve sensitive data, Port 43 should be available to Registrars solely for the purpose carrying out its obligations with respect to transfers of domain names between registrars.

7. Automated Access to Whois

Some members of the Task Force stated that they may not be fundamentally opposed to having an automated mechanism to retrieve Sensitive Data for approved Requestors with approved purposes provided that:

- The Requestor is asked to sign (or "click") an electronic license agreement for the Sensitive data promising:
    - To use the data for only the purpose(s) indicated;
    - That the Whois data will not be used for marketing purposes; and
    - That the Requestor shall be prohibited from compiling, leasing, sublicensing, reselling or otherwise transferring the data to any third party (except to comply with law).
- The Requestor is identified to the Whois Provider;
- The Requestors identity and purposes for such information is disclosed to the Registrant.
    - The group recognizes, however, that an exception may need to be granted for certain law enforcement investigations (including civil investigations), only when notification of the registrant will defeat the purpose of the investigation.
- The Sensitive Data is provided to the Requestor in human-readable format only (and not computer readable).

8. Approval Process for Automated Searches to prevent data mining

If there were to be an automated process available to retrieve sensitive data, like that currently provided under Port 43, with the functionality described in Section 7 above, the group discussed two alternative methods of regulating access to sensitive data

White List. One would have a central authority (not a registry or registrar) approve entities that could

use this automated process. This option became known as a "White List" of IP addresses. In this scenario, a White List would be created of Requestors that are believed to be nonmarketing users of Whois information (i.e., Law Enforcement, Consumer organization, Intellectual Property Organizations, etc.) This list would be provided to the registries and registrars and only those Requestors sending requests through the automated process would be allowed to access the sensitive Whois information. Questions arose concerning (a) who would operate this White List, (b) what would be the criteria for being on this White List, (c) whether it was actually feasible to implement; (d) secondary use of access, and (e) a process for dealing with abuses.

Individual Use List. The other alternative would approve specific individual uses of sensitive Whois data rather than giving blanket approvals to user entities. Each time a requestor wanted to gain access to Whois information it would submit an automated request to the Whois Provider. The Requestor would identify itself to the Whois Provider and also identify the specific purpose for which the data was requested (i.e., suspected trademark infringement, a desire to contact the domain name holder for sale of the name, suspected consumer fraud, etc.). This option would give all Internet users the same rights to access sensitive Whois data, but would require them to authenticate their identification. It would also require the creation of a "list of approved purposes" as described above.

A minority of the Task Force constituencies, including those representing the Noncommercial Constituency and the At-Large Advisory Council believe that the creation of a White List would be impractical and would place a large burden on the entity handling requests to be on the White List. In addition, they do not believe that any Requestor should be entitled to the Sensitive Data unless retrieval of such information was pursuant to a formal request by law enforcement (i.e., subpoena).

A majority of the Task Force constituencies, including those from the Commercial and Business users, ISPs, gTLD Registries and Intellectual Property Owners do not fundamentally oppose the “White List”, but believe that it is essential for those legitimate Whois users to obtain the Sensitive Whois information in a timely and reliable manner. Moreover, these representatives questioned whether the cost of implementing such a system would be one which could be borne by the current funding models, and encourage that a cost-benefit analysis be undertaken before any such system is approved and implemented.

Finally, if there is a “White List” or “Individual Use List,” the Task Force emphasized the need that a mechanism be employed to authenticate the identity of the Requestor to the entity administering either alternative.

With respect to the alternatives presented above, the Task Force seeks comment on this entire section, including the following questions:

- If there were a White List or Individual Use List, who would serve as the central authority ("Authority") that determines the eligibility for entities to be on these lists?
- Does this same Authority maintain the centralized white-list or Individual Use List database/system?
- What are the criteria that the Authority uses to determine who is eligible to be on either list?
- Is there a limit of the number of entities that can be on the White or Individual Use Lists?
- Who pays for the implementation of either system? Would there be a contribution paid by the members of the either list?
- If entities on the White or Individual Use List must give the reasons for their queries, how does (or can) that information be delivered to the registrants?

Other Considerations

10. A technical means of providing this tiered access (i.e., allowing these parties to access the information, while preventing others from getting the information) could be through the IRIS protocol developed by the CRISP working group of the IETF. When finalized, we believe that a comprehensive

review of this technical solution be undertaken. We believe a more detailed effort is needed to identify any specific parties that need access to selected elements and what information should be obtained about such access.

11. A Cost benefit analysis should be done when considering any significant changes in Whois requirements. Such analysis should include how the costs are distributed and who bears such costs.

12. Finally, careful consideration should be given to the feasibility of registrars and registries to implement any proposed changes in Whois requirements including but not limited to enforcing such requirements. And sufficient time should be allowed for any associated migration.

http://gnso.icann.org/issues/whois-privacy/Whois-tf1-preliminary.html#PolicyRecommendations

Whois TF2 – Tiered Access related recommendations

3.5 Publication of Data

The task force believes that a system that provides different data sets for different uses (also known as "tiered access") may serve as a useful mechanism to balance the privacy interests of registrants with the ongoing need to contact those registrants by other members of the Internet community. The task force believes that such a system should be based on the following principles:

a) Technical and operational details about the domain name should continue to be displayed to the public on anonymous basis. Providing some basic contact information (possibly limited to the name and country for both the registrant and administrative contact) may also be appropriate in the interest of balancing contactibility and privacy concerns for publicly available information. Further contact details for the registrant and administrative contact would only be available in one or more protected tiers.

b) Registrants should have the option to direct that some or all of their protected data be displayed to the public.

c) Those meeting the requirements and identifying a legitimate use to access protected information should be able to obtain it in a timely manner.

d) Those seeking access to protected information should identify themselves in a verifiable manner. Once identified, the user would be issued a portable credential, rather than needing to verify their identity on a registrar-by-registrar (or even registry-by-registry) basis.

e) The system should be affordable, both for implementers and users.

f) Registrars and registries should continue to have full access to the WHOIS data for technical and operational purposes.

However, the task force also identified several questions that still must be answered before a tiered access system can be implemented. Specifically:

a) What process of notification to registrants, if any, should take place when their protected data is accessed other than in circumstances required by law or contract (e.g. the provision of contact to UDRP providers during a UDRP dispute, or to another registrar during a transfer)?

b) What contact data should be shown in the protected tier? How will the data compare with what is now available? How will the accuracy compare with what is now available?

c) What are the mechanisms available for identifying and authorizing those requesting access to protected information? Are those mechanisms fast? Are they affordable? Are they online? Who will administer them, using what criteria?

d) How will the costs of implementing a tiered access system be borne?

e) Will existing technology standards (such as CRISP) would support such a system? If so, how?

http://gnso.icann.org/issues/whois-privacy/Whois-tf2-preliminary.html#PublicationofData3