STAFF IMPLEMENTATION NOTES

WHOIS Working Group Report

11 October, 2007

Status of the Document

Final Staff Implementation Notes for GNSO Council consideration.

Summary

This document contains Staff Implementation Notes on the WHOIS Working Group Report, prepared as requested by the GNSO Council Resolution of 6 September, 2007.

Prepared by Liz Gasster
policy@icann.org

Staff Implementation Notes on WHOIS WG Report
Author: Liz Gasster (in consultation with Legal and Services Staff), policy@icann.org

Page 1 of 17

Date:

10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

Contents

Date:
10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

Introduction

The following is an assessment of issues and implementation options relevant to implementation of a new OPOC position. This assessment addresses each of the three areas that the GNSO asked the WHOIS Working Group (WG) to consider, reprinted below, and also adds a fourth area of staff review, which considers the studies called for in Section 8 of the WG Report.

1. to examine the roles, responsibilities and requirements of the OPOC, and what happens if they are not fulfilled (see Section I);

2. to examine how legitimate interests will access registration data no longer published via WHOIS (see Section II); and

3. to examine whether publication of registration contact information should be based on the type of registered name holder (legal vs. natural persons) or the registrant's use of a domain name (see Section III).

The WG Report notes that implementing an OPOC would change the way certain data is collected, displayed and accessed, resulting in increased costs for service providers (WG Report, Sec. 1) and delays for requesters of unpublished WHOIS data, compared with the status quo (WG Report, Sec. 3.1). These implications are highlighted where applicable below.

Staff's implementation assessment (all staff comments provided below) also recognizes these same implications. As the Working Group considered how OPOC would work, it discussed various mechanisms that might be implemented to improve how OPOC might work or address various aspects of OPOC. Examples include mechanisms to be sure an OPOC's email is valid, mechanisms to demonstrate affirmative consent by OPOCs, and mechanisms to provide direct access to unpublished data from registrars in certain instances. In each case, mechanisms thought to be essential by some WG participants were rejected by others. In considering these and other "implementation options" identified by the WG, staff notes that implementation of each mechanism contemplated by the WG may have certain benefits (for example enhancing accuracy or reliability), but may also add complexity, cost, or create other potential challenges (for example time delays) to OPOC's implementation. For these reasons it might be useful to consider implementing OPOC in a "streamlined" rather-than "full blown" way. A streamlined implementation might eliminate or minimize any required verification or consent, and accept self-attestation for direct access (from a registrar or registry) in lieu of an automated authentication mechanism. A more robust, "full-blown" OPOC implementation might require automated OPOC email verification and affirmative consent to the registrar, and fully authenticated access to unpublished WHOIS data. Of course each option has important consequences including questions of cost, accuracy, reliability, timeliness and recourse. Considering the issues identified by the Working Group, staff notes the difficulty involved in formulating an implementation of OPOC that would address all stated concerns.

Staff also recognizes the absence of a contractual relationship between ICANN and the OPOC. If OPOC were implemented, ICANN would have no mechanism to assure compliance or provide recourse. The following graphical representation of ICANN's contractual relationships illustrates this issue. Another "streamlined" implementation of OPOC might limit the entities who may be an OPOC to either a registrant or registrar. In each of those cases there is an existing contractual relationship which can be enforced. This concept is described further below.

Date:
10/12/2007

**Staff Implementation Notes
WHOIS Working Group Report**

ICANN & Contractual Relationships
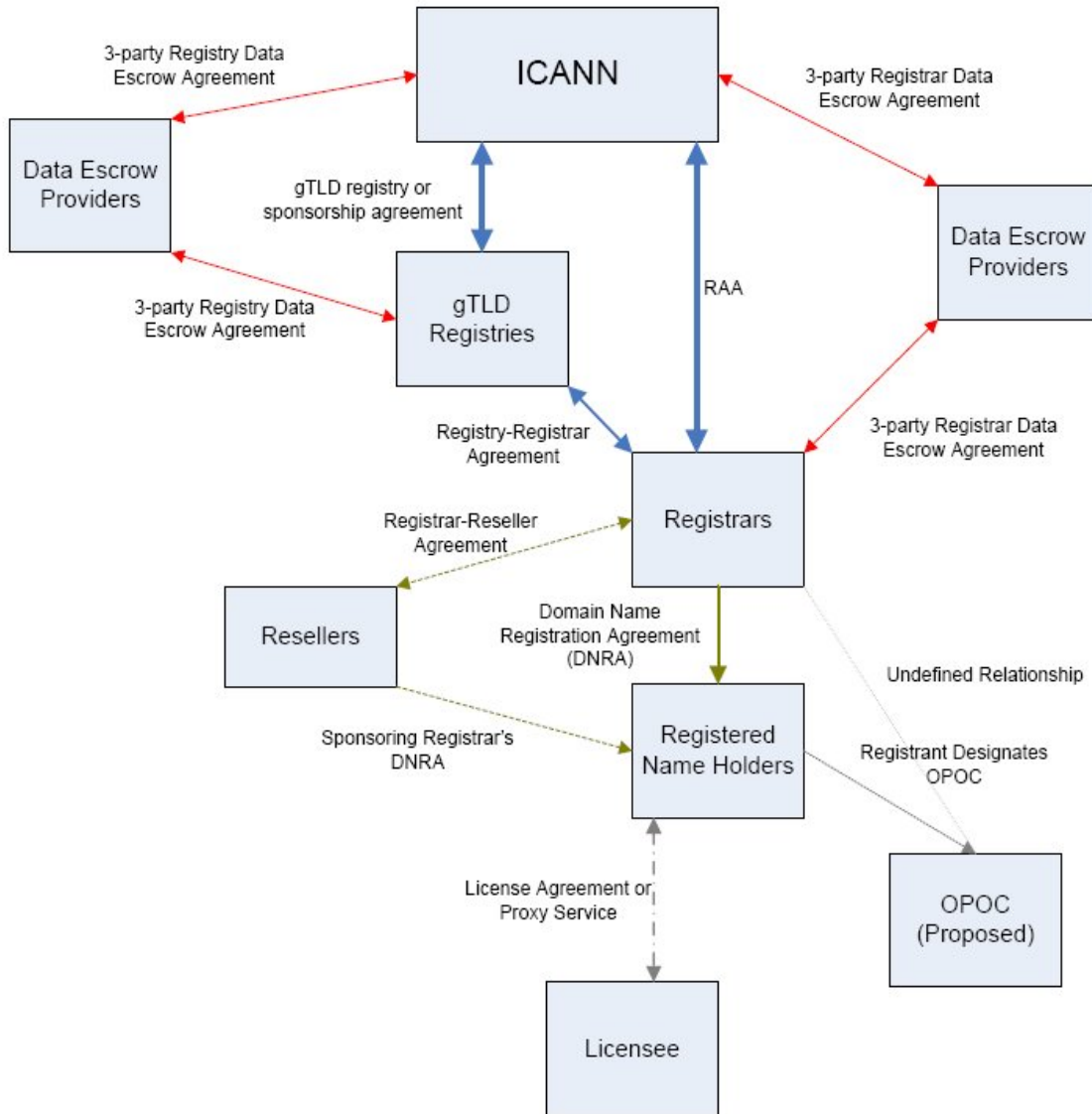
Date:
10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

Note about the approach taken in this document: The WG Report itself highlights key implementation options identified by participants. These implementation options are reprinted below and identified as "Implementation options Identified by the WG". Staff notes are identified as "Staff assessment".

I. Defining the roles, responsibilities and requirements of the OPOC, and what happens if they are not fulfilled

A. Examination of role and responsibilities of the OPOC (WG Report Section 3)

The purpose of the OPOC is to provide a point of contact in lieu of the registrant. The WG Report identifies three roles the OPOC might perform:

1. To *relay* requests in a timely manner and meet certain key implementation requirements (3.1)

2. To *reveal* unpublished information about natural persons in a timely manner when there is reasonable evidence of actionable harm; or reasonable evidence of inaccurate WHOIS data; or when relay fails after a specified period of time (3.2)

3. To determine and implement a *remedy*, but only when the registrant consents (3.3).

1. Relay:

Implementation options Identified by the WG regarding the RELAY function (3.1):

- How to assure immediate response by the OPOC on a 24x7 basis?

- Possible automatic real-time forwarding of e-mail requests from requester to registrant

- Possible automatic real-time forwarding of responses from registrant to requester

- Capability to forward requests and responses in other formats (e.g. fax or post)

- Responses from registrant to OPOC should also be forwarded to requester immediately.

- Regarding good faith vs. bad faith requests -- Requesters of contact information might be required to indicate the reason for the request such as: a reasonable suspicion of (check one):

  - fraudulent activity

  - intellectual property infringement

  - false declaration as a natural person

  - inaccurate WHOIS data

  - other legal infringement (specify)

  - other e.g. good faith (specify)

Staff assessment re: Relay: Staff has considered the role of an OPOC to relay requests to a registrant, and agrees that the relay function could be implemented in such a way that an OPOC would not be obligated to relay without the requester providing some of the substantiating information listed above. However, staff notes that ICANN may have no way to assure that the OPOC does relay,

as ICANN currently has no contractual relationship with the OPOC. ICANN would have to enter into contract with the OPOC, and the specifics of compliance would depend on what obligations are imposed and how. Absent recourse or an enforcement mechanism of some kind, if an OPOC were to fail to respond, a registrant could lose a domain name.

One possible alternative may be to require the OPOC to be the registrar if the OPOC is not the registrant. In this scenario, the OPOC's responsibilities could be imposed indirectly through the domain name registration agreement. It is difficult to envision any requirement that could be drafted that would be enforceable by ICANN without a contractual relationship.

Implementing the roles of the OPOC as discussed by the Working Group may require significant resources. A third-party OPOC that is not the registrant or the registrar may have difficulty providing 24x7 response and real-time forwarding, unless the third-party OPOC is in the business of being an OPOC (such as a proxy service). Some registrars will be better able than others to provide 24x7 real-time forwarding on an immediate basis.

2. Reveal:

Implementation options identified by the WG regarding REVEAL (3.2):

- If Registrant response is not received promptly (perhaps 12 hours after an e-mail request has been forwarded), OPOC may try to contact the registrant using all available means (e.g. telephone).

- If no response is received within 72 hours, the OPOC may be required to reveal registrant contact data immediately to the requester.

- Existing provisions in certain Registry agreements may provide an implementation solution.

- The following may require more definition:
    - Reasonable evidence of actionable harm
    - Reasonable evidence of inaccurate WHOIS data
    - When relay fails after a specified period of time

Staff assessment re: Reveal: The original OPOC proposal stated that "The purpose of the OPOC is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name." Under this definition, an OPOC would be expected to relay inquiries about a domain name registration to a registrant. It is not clear from this definition whether the OPOC was envisioned to have the responsibility to reveal the underlying registration data to a requester.

It is unclear how the first two bullet points above can be enforced. In addition, even if OPOC implementation were limited to registrars, more specificity would be needed to determine the conditions under which a registrar (or registry) would be obligated to reveal the underlying registration data in situations where the relay option did not result in a response from the registrant (see also staff notes regarding access to data from registrars and registries, Section II below).

3. Remedy

Implementation options identified by the WG regarding REMEDY (3.3):

- Implementation is out-of-scope. Remedy involves OPOC interaction with ISPs – noted because it is a role of the OPOC and in the scope of the GNSO.   It is unclear how this responsibility can be implemented.

- Timely may be interpreted as a time line that is proportional to the harm.

Staff assessment re: Remedy: The Working Group decided this area was out of scope and therefore Staff has no notes on this option.

B. Examination of characteristics and requirements of the OPOC (WG Report, Section 2)

The WG agreed on several characteristics of the OPOC. For example, there may be up to two OPOCs; the OPOC may be a registrant, registrar or third party appointed by the registrant; and all registrants (legal and natural persons) must appoint an OPOC. The OPOC would have a consensual relationship with the registrant and defined responsibilities. The WG also agreed that implementing an OPOC may simplify contact information currently displayed in WHOIS.

Implementation options identified by the WG (2.2):

- There will need to be a change to both the Registrar Accreditation Agreement (RAA) and subsequently Registrar-Registrant agreements to reflect a new OPOC relationship.

- It is not intended that the implementation of OPOC need create any particular legal relationship that may exist in national law other than an enforceable contract.

- There may be a need to change data fields in the public display of WHOIS information in Registry agreements.

Staff Assessment re: OPOC characteristics and requirements: This section contemplates a contract between the registrant and the OPOC. One way of simplifying the implementation of OPOC might be to consider allowing only registrants or registrars to be the OPOC. ICANN could require the registrar to require the registrant to require the OPOC to follow certain obligations. However, based on the language of this section, staff does not understand the Working Group's position on the relationship between the registrar and the OPOC. If the registrar is the OPOC, the registrar has a contractual relationship with ICANN. If a third party is the OPOC, then no contractual relationship exists.

Changes will be needed to the public WHOIS provisions in the gTLD registry agreements, and these changes should be resolved prior to the launch of the new gTLD process. If changes are made to the fields of information displayed in WHOIS, these changes will impact the current escrow of registrant data. Third party data escrow providers may have to alter their protocols to remove the admin contact (or any other fields that are changed).

Staff also notes that the original OPOC proposal would appear to make all registries thin registries. Implementing this aspect of the OPOC proposal would eliminate the possibility that registry WHOIS could provide a backup to registrar WHOIS if needed. For example, in the case of RegisterFly, the registries that had thick WHOIS were able to recover information on domain names under RegisterFly's management more quickly than .COM/.NET (which are thin registries and did not have the underlying WHOIS data, which was held by RegisterFly). If a registrar fails, thick WHOIS may be important for registrants.

Staff is also not clear on how the OPOC proposal would be implemented on the 100+ million existing domain name registrations. How much time would be provided for registries and registrars to implement the contemplated changes? Would it be the responsibility of registrars to inform their customers of the changes? Is implementation expected to occur only for new registrations and renewals, or must all current registrations be updated to provide OPOC information?

1. Verification of OPOCs (2.3)

The WG considered the need to verify the e-mail address of the OPOC to ensure functionality. While the WG rejected centralized accreditation of OPOCs as neither scalable nor practicable, there was support for verification of the OPOC's e-mail address. There were also concerns associated with such verification, including the cost to Registrars and the timing of when verification should occur, if implemented.

Implementation options for verification identified by the WG:

- Verification could be done by requiring a reply to an auto-generated e-mail.

- Verification may be obtained at the same time as consent (see below)

- The name may be put on hold status by the registrar pending verification and then put on active status.

- Registrars may engage with registries with respect to hold status.

- Where registration is not bound to subsequent web-site activation, no process will be required.

Staff assessment re: verification -- Registrars are not currently required to verify the email address of a registrant or admin contact, so contractual conditions would have to be imposed to require verification of the email address of an OPOC. This could be manipulated easily by OPOC registrars.

It is important that feasibility studies be conducted to better understand the impact of this recommendation on the current registration process. A feasibility study may be costly and take several months to complete.

If the registrant is a legal person, then current information displayed in WHOIS remains the same. Full contact data should be available. The legal- vs. natural-person distinction would not necessarily turn all registries into "thin" registries. If the registrant is a natural person, then either partial information (registrant name and jurisdiction), or OPOC full contact data can be displayed or refer the requester to contact the registrar or registry for special access to full data. The registrant could also opt-in to WHOIS and have full information displayed.

2. Consent to be an OPOC (2.4)

The WG also considered whether an OPOC needs to provide consent. The WG agreed that the registrant is responsible for naming a functional OPOC and that a process to establish the consensual relationship between the OPOC and the registrant is required. While there was agreement that a process to establish the consensual relationship between the OPOC and the registrant is needed, there were differing views about when and how consent might be obtained, and some concern about the burden that an explicit consent requirement might place on both registrants and registrars. There was also an issue about timing, and whether registration should be allowed to complete before consent is obtained.

Implementation options identified by WG participants:

- Consent may be obtained by requiring a reply to an auto-generated e-mail (via e-mail or a web-based agree system) at the same time that the OPOC e-mail address is verified.

- The name may be put on hold status by the registrar pending OPOC acknowledgement.

- Registrars may engage with registries with respect to hold status.

Date:
10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

- Registrars may need to consider changes to billing functions.

- If more practicable, the responsibility for "the process of consent" could lie with the Registrant and be regulated within the Registrar-Registrant agreement.

Staff assessment re: consent: Requiring consent by the OPOC to be an OPOC could be part of the registration process, but may be manipulated easily and could introduce unintended consequences.

Feasibility studies may provide insight on how consent can be implemented.

Regarding changes by registrars to billing functions -- the costs of implementing consent should be studied.

Changes will be needed to both the RAA and registrar-registrant agreements to reflect this relationship. There may also be a need for changes to the fields of data in the public display of WHOIS information in registry agreements.

3. The OPOC and tech/admin contacts

Implementation options identified by WG participants:

- Consideration should be given to merging the admin and OPOC.

- Consideration should be given to reconciliation of different display obligations between registries and registrars.

- In pursuing simplification, national legal obligations may need to be considered.

Staff Assessment re: OPOC and tech/admin contacts: Reconciliation of the different display obligations between registries and registrars would have to include discussion of display differences between thick and thin registries, and respect national laws obligations. This can be accomplished but the final policy adopted should allow for some minor differences in the display obligations depending on national laws and registry structure. This would also involve changes to data escrow requirements and protocols, data escrow provider notification and alterations of the storage of escrowed data.

C. Examination of what happens if the OPOC's responsibilities are not fulfilled (WG Report, Section 4)

The WG considered the compliance and enforcement aspects of the OPOC proposal and the issues that arise when an OPOC fails to fulfill a designated role or responsibility. The WG agreed that when an OPOC fails to act or to act within a designated time to fulfill a relay or reveal request, the Requester may contact the Registrar directly.

Implementation options identified by WG participants:

- Registrars may require certain proof of the OPOC's failure from the Requester.

- The name may be available for resale after 90 days.

- Registrars may establish appeals or dispute resolution mechanisms whereby the Registrant may object in a timely manner to any of the above actions.

Staff assessment re: failure of OPOC to fulfil a designated role or responsibility: The actions taken when an OPOC fails to fulfil a designated role depend on whether the OPOC is the registrant, registrar or a third party. ICANN has an agreement with the registrar and the registrar has an agreement with the

registrant. As mentioned previously, currently ICANN does not have a relationship with the OPOC, unless it is the registrar or registrant.

II. Examining how legitimate interests will access registration data no longer published via WHOIS (Section 3, Section 5, Section 6)

If the OPOC proposal is implemented, requesters of information about natural persons would typically contact the OPOC to relay requests and/or reveal information. In addition, the WG also considered the circumstances under which unpublished WHOIS data might be accessed directly from a registrar. The WG discussed whether access should be limited to certain entities, and whether various entities should be allowed different types of access. The WG considered four types of access (Section 6):

    a. Access to displayed WHOIS records (6.1)

    b. One-time access to a specified un-displayed data record (6.2)

    c. Regular query-based access to un-displayed records (6.3)

    d. Full access to displayed and un-displayed records (6.4)

A. Access to displayed WHOIS records (6.1):

Access to displayed WHOIS records would continue and would result in access to the full data records for legal persons and to limited data records for natural persons.

B. One-time access to a specified un-displayed data record (6.2):

This access would take place when there is "reasonable evidence of actionable harm". This access would need to be timely to be effective.

Implementation options identified by WG participants:

- Regarding timeliness -- Timeliness may be defined as proportionate to the suspected harm and related to the means of access.

- Existing provisions in certain Registry agreements may provide an alternative implementation option

C. Regular query-based access to un-displayed records (6.3)

This access would take place when there is "reasonable evidence of actionable harm".

Implementation options identified by WG participants:

- A pre-registration system by registrars for those allowed direct access (referred to as "accessors") may be needed.

- A restriction of the number of queries available in a certain time period may be imposed on accessors.

- There may be a need for record keeping of queries by the registrar.

- There may be means to sanction accessors for abuse of limitations.

- Limitations may be specified in contractual conditions agreed between accessors and Registrars.

- Existing provisions in certain Registry agreements may provide an alternative implementation option.

D. Full access to displayed and un-displayed records (6.4)

Implementation options identified by WG participants:

- Data records may be encrypted and a key supplied

- Data records may be in a password-protected database and a password supplied.

- Existing provisions in certain Registry agreements may provide an alternative implementation option.

E. Implementation of access (6.5):

While WG members agreed about certain instances in which LEAs and private actors should have direct access to unpublished WHOIS data via registrars, these views were not consistently held across constituencies (Sec. 6.5).

Implementation option identified by WG participants:

- The "circumstances" for allowable access need to be consistently defined.

Staff Assessment re: Access:

ICANN would not be able to require an OPOC to reveal information unless it is the registrar. Reveal can be accomplished by access to a registrar or registry.

Requesters may choose to obtain information directly from the registry rather than contact the registrar. The WG report focuses primarily on accessors contacting registrars, but accessors could also contact registries to obtain the information.

Registrars may provide an access method, but this may come with a fee. The fee may be necessary to verify the address of the requester and serve as deterrent to data mining.

Registrars have historically been reluctant to release information without some form of indemnification against possible lawsuits. – this is particularly true when confidential registrant information is involved.

Would registrars be expected to provide encrypted access to non-public data? This requirement will impose costs on registrars. Some registries already have a system for encrypted tiered access. Registrars could offer such a service.

F. Authentication (6.6):

The WG considered whether registrars should authenticate parties requesting access. The WG Report notes concerns that authentication would introduce delays and impose cost. The WG identified two potential authentication mechanisms, self-declaration and third party authentication. The WG knew of no instance of a globally scalable system of authentication and concluded that the practicability and cost-effectiveness of authentication should be an area of further study (see also Section 8). In the absence of a better option, there was support for adoption for "self-declaration" along with safeguards to prevent abuse. Others viewed self-declaration as insufficient and stressed the need for authentication.

Implementation options identified by the WG regarding authentication:

- Self-declaration by the accessor could be backed up by a challenge procedure by the registrar, signed affidavit from the accessor, and/or penalties for misrepresentation.

- Private actors may enter into agreements with a registrar to enable or speed access.

- For self-declaration to be subject to an effective challenge procedure, work may be needed to determine "effective".

- A specific means of access for the banking sector should be considered.

Staff assessment re: Authentication: Authentication may be addressed through access, and depends on the form of agreement and conditions for access to non-public data.

G. Charging for access services (6.7)

Implementation option identified by the WG regarding authentication:

- Registrars may consider charging a nominal fee for Access services.

Staff assessment re: fees for access: .NAME charges a nominal fee for access to non-public records through their Detailed Access service, and Telnic is proposing a similar fee for access to non-public records for natural persons through their Special Access Service. If OPOC is implemented, registrars may consider charging a nominal fee for access to non-public data. A cost analysis may be necessary.

III. Examining whether publication of registration contact information should be based on the type of registered name holder (legal vs. natural persons) or the registrant's use of a domain name (Section 5)

The WG agreed that the OPOC proposal should change WHOIS policy on publication of data to distinguish between natural persons, where there would be only limited public display of WHOIS records, and legal persons (company, business, partnership, non-profit entity etc) for which there would be full display. However, the WG felt that a distinction based on use was neither sufficiently timely at the point of registration nor easily operational.

Implementation options identified by WG participants:

- A checkbox (to select natural or legal) could be part of the registration process.

- The existing flag facility within the Extensible Provisioning Protocol used by registries and registrars may be a basis for implementation.

Staff assessment re: Distinction between natural and legal persons:

This will have an impact on the RAA and registry agreements. Only two registry agreements currently provide for differentiation in short and full format, but none provide for differentiation between natural persons and legal persons. Nominet (the .UK registry) requires registrants to designate themselves as UK-based trading entity, a non-trading UK individual or a non-trading, non-UK individual.

IV. Feasibility studies (Section 8)

The WG Report suggested ICANN staff conduct four feasibility studies related to the OPOC proposal described in the Report.

1. Cost-related studies

- Costs to implement verification and consent (section 2.3 and 2.4).

- Costs to implement compliance (section 4).

- Costs to implement the access options (section 6).

- Marginal costs to implement a new fee-based system for accessors compared with recovering additional costs from user fees using existing systems.

Staff assessment:

Staff recommends that studies related to costs of implementation of a new WHOIS policy be contingent upon completion of the research described in point "4" below, assuming the results of that research demonstrate need for additional research. While some have referred to this step as a "cost/benefit" study, strictly speaking, only costs and not benefits would be considered within the parameters of the studies described.

2. Study of data privacy issues arising from self-declaration of Accessors (see section 6)

Staff assessment:

Staff recommends that studies related to data privacy issues arising from the self-declaration of accessors in the access proposal be contingent upon completion of the research described in points "4," "1," and "3," assuming the results of that research demonstrate need for additional research.

The application of ICANN's consensus policy regarding conflicts between WHOIS requirements and national/local laws could impact or potentially obviate the need for research in this area since registrars and registries affected by privacy laws could potentially effectively opt out of contractual WHOIS requirements.

3. Study of mechanisms for a practicable, cost-effective, globally scaleable means of authenticating accessors (section 6)

Staff assessment:

Staff recommends that studies related to a globally scalable authentication of accessors be contingent upon completion of the research described in points "4" and "1," assuming the results of that research demonstrate need for additional research.

Substantial consultation will be required in order to define an "accessor" and identify/clarify credentialing requirements, particularly in collaboration with the GAC, as this body may provide useful input regarding how to define this concept in a manner that is representative and respectful of varied national practices and structures.

A registrar or registry may implement a secure system and require accessors to sign an agreement and provide verifying information. The registrar or registry could send a pin # and login to the accessor for use of the secure system. If the registrar or registry determines that an accessor submitted false information, then the agreement can be rescinded and the accessor will be considered to have breached the agreement.

4. Study on information on gTLD registrants and registrations and the use and misuse of WHOIS data.

Staff assessment:

On 6 September, 2007, the GNSO Council approved a resolution that, among other things, directs staff to implement an expanded version of this study, to also include a review and analysis of proxy services that are currently available. As requested by the GNSO resolution, staff prepared a report on the "study to date" on 4 October, 2007. Staff's report identified several questions about the scope and details of the study envisioned by the GNSO Council and requested further guidance from the Council before engaging in such a study. The relevant text of the GNSO Resolution and ICANN staff's report on the "study to date" is extracted for ease of reference below.

In addition to the questions and comments set forth below, staff recommends that studies related to use and misuse of WHOIS data precede the other identified areas of research.

ICANN's Contractual Compliance department is conducting an audit related to WHOIS data accuracy that will involve sampling of data to estimate extent of WHOIS data inaccuracy. A study of this nature would not, however, address the impact of changes to the WHOIS system or implementation of a new WHOIS policy; rather, it would measure or approximate percentages of inaccuracy among WHOIS data.

Even with the results of a statistical analysis that attempts to quantify the level of inaccuracy, this sort of analysis would not assess the "costs" associated with inaccuracies in WHOIS data, or, put in other terms, it would not assess the "benefit" of undertaking efforts to correct inaccuracies.

Excerpted Text of GNSO Resolution requesting a study on WHOIS:

"The GNSO Council] requests ICANN Staff proceed with a study of gTLD registrations and registrants and how WHOIS data is used and misused as described in the GAC Principles Regarding gTLD WHOIS Service paragraph 4.2, and by the Working Group Final outcomes report. This study should include a review and analysis of the different proxy services available today and a summary of any other statistical studies that Staff can locate. We ask staff to report back to the council on the 'study to date' by October 4."

Staff assessment reprinted from the Staff Report on the WHOIS "study to date" provided to the GNSO Council on 4 October, 2007:

This is broad language and is subject to interpretation in terms of the scope of what is actually being called for. Staff assumes (but would welcome confirmation) that the GNSO Council intended to call for four distinct study components, as follows:

1. A "study of gTLD registrations and registrants" --

Scope of study -- How should the scope of this study be defined? What does the GNSO Council want to know about registrations and registrants? Possible characteristics the Council might want to know include:

- The GNSO Council may want to know how many registrants are natural persons (real, living individuals) vs. legal persons (business, association, non-profit, etc.).

Date:

10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

- o GNSO might consider studying only those gTLDs that have registrants who are natural persons
  - o Guidelines would need to be developed to specify how determinations of legal vs. natural persons would be made and there would be some margin of error
  - o The GNSO Council might consider sorting registrants who are natural persons by country
- The GNSO Council may want to know how accurate registration data is. If so, an ICANN WHOIS Compliance audit is underway, and is assessing questions of accuracy. However, this is the first audit of its type. An update will be provided in LA, but comprehensive data may not be available for some time.
- The GNSO Council may want to know the percentage use of proxy services and privacy services among all registrants.
- What other characteristics of registrations and registrants should be studied?

Other study options and considerations:

- A 2005 study by Verisign (see attached "summary of Whois data points') has data about natural vs. legal persons in .com and .net.   Is this kind of data what the GNSO Council is seeking?

Staff recommendation:

- The GNSO Council should provide any further guidance to ICANN staff as to the information about registrations and registrants that is being requested.
- Staff should consult with internal subject matter experts, a knowledgeable statistician (or study "designer") and external stakeholders about what specific characteristics of registrations and registrants should be studied. Are the characteristics suggested above correct?
- Staff should work with experts as needed to develop cost and time-frames for delivering such a study.
- Staff should respond to the GNSO Council with a specific study recommendation, based on the preceding, and any other useful data. At that time staff may also determine anticipated costs and time frames for completion.

2. A "study of how WHOIS data is used and misused" –

Scope of Study -- What does the GNSO Council want to know about uses and misuses of WHOIS query data?

Study options and considerations:

From a qualitative perspective, there are a number of existing references that describe uses and misuses of Whois data.   Several useful documents identify and describe ways in which Whois data is used to support both "legitimate" and "illegitimate" activities. For example, the GAC Principles enumerate many ways that Whois data is used in support of legitimate activities. One possibility is that ICANN staff could use resources such as the GAC Principles as a foundation to develop a compendium of different uses and misuses of Whois. Such a compendium might be a useful set of descriptions but would not provide insight into relative volumes or the scope of various types of misuses.

It is difficult to gather and analyze accurate quantifiable data about the uses and misuses of Whois query data. The quantitative data we do have is more limited. A recent SSAC spam study focuses on just one

Date:
10/12/2007

type of misuse of Whois data, and points to evidence that Whois queries are misused by spammers to harvest email addresses, but there currently is no public data that analyzes the purposes or amounts of various data queries overall. A 2002 study, the "Whois Survey Report", identified in the recent summary of available Whois data points compiled by ICANN staff, examined over 3000 Whois queries in an effort to understand better who uses Whois data and for what purposes. Though the 2002 survey provides interesting insights about users of Whois, the report's authors caution repeatedly that the study is neither statistically valid nor definitive.   If ICANN staff were to initiate a similar survey, we would need to consider potential challenges and any limitations of such an approach. One possibility is to craft a survey that registrants complete when registering for a domain name, similar to the one employed in the 2002 Whois Survey Report. We would likely need a willing registrar or two, or registries, to participate, and the data would be self-reported, a limitation given the need to understand misuses of data which would not be captured by self-reported data.

Alternatively, we could consider developing an independent study (one not dependent on self-reported data), but the feasibility of such a study would need to be studied further. Such a study would require a larger budget and could take several months to design and implement. Expertise would be needed as to how this might be done without relying on self-reported data regarding misuses.

Summary of above – three possible options (any/all could be refined further as requested):

2.1 – Compile descriptive compendium of uses and misuses of Whois data
2.2 – Work with willing registrars and registries to conduct a survey of those who use Whois data. Caveat: need willing service providers
2.3 – Work with an independent study expert to design and implement a study of uses and misuses of Whois data. This study might also benefit from use of data from willing registrars and/or registries.

Staff recommendation:

- The GNSO Council should provide further guidance about the scope and approach to the study it envisions.
- Staff would scope further (cost, timeline) following GNSO guidance.
- Implement as requested.

3. A "…review and analysis of the different proxy services available today" –

Scope of study --

- The GNSO Council has requested that staff examine proxy services – (proxy: when a party enters into an agreement with a registrar and becomes the registrant as a proxy for a beneficial user). Numerous companies act as proxy registrants, including web design firms, law firms, marketing firms, web hosts, registrar subsidiaries, resellers and individuals. The "proxy" serves as the registered name holder, and the domain is then licensed to the beneficial user. Section 3.7.7.3 of the RAA[1] addresses this scenario.

_____

[1] *3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact*

Date:
10/12/2007

Staff Implementation Notes
WHOIS Working Group Report

- The GNSO Council may also want to examine other privacy services, such as registrars or resellers that supply customers with alternate contact information and a mail forwarding service while leaving their customer identified as the actual registered name holder.
- The GNSO Council might consider a review of any terms of service that might be of particular interest, such as a review of provisions which describe the circumstances under which personal contact information of a registrant might be revealed.
- What is the information we want to have about the different proxy services available today?

Staff recommendation:

- The GNSO Council should provide any further guidance on the scope and details of the study requested.
- Staff will proceed with review and analysis of proxy services available today by engaging a researcher to perform an analysis of the proxy marketplace.
- Staff will provide a time frame for completion once the GNSO Council confirms the scope of the study requested.
- Note also the suggestion made in Study # 1 above that quantifiable data be gathered about the use of proxy services as part of a study on registrations and registrants.

4. **"summary of any other statistical studies that Staff can locate"** –

Staff recommendation: Staff plans to provide an updated version of the "summary of available WHOIS data points.

information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm.