Draft Outcomes Report of the Whois Working Group

STATUS OF THIS DOCUMENT

This is Version 1.5 of the Outcomes Report of the Whois Working Group.

TABLE OF CONTENTS

INTRODUCTION

Status of statements in this report and description of consensus-building conventions used

Unless otherwise stated, every statement in this report is an agreed description or assertion of the WHOIS Working Group. Some statements are preceded by the term '*AGREED'* . These statements are an agreed policy recommendation of this group. Some statements are qualified by a characterisation of '*SUPPORT'* or '*ALTERNATIVE VIEW*'.

The Working Group used the following conventions to express or move towards consensus:

- **Agreed** – there is broad agreement within the Working Group though not necessarily unanimity
- **Support** – there is some gathering of positive opinion, but competing positions may exist and broad agreement has not been reached
- **Alternative view** – a differing opinion that has been expressed, without garnering enough following within the WG to merit the notion of either Support or Agreement.

Implementation options are shown in box. These are intended to be addressed by ICANN staff or third parties after completion of the tasks of this working group.

The ultimate authority to determine the level of agreement was that of the Working Group Chair, Philip Sheppard, assisted by the Vice Chair, Jon Bing.

SECTION 1 OBJECTIVE

Balancing personal privacy and public interest

In discussing the OPOC proposal the working group was broadly seeking an outcome that would improve certain data privacy aspects of WHOIS services, while simultaneously improving the ability to address issues relating inter alia to the public interest, consumer fraud and other acts of bad faith by Registrants.

The essence of the underlying debate was the exceptions when it is necessary to enable activities in pursuit of the prevention of criminal or civil harm. In this pursuit it is understood that there are exceptions when the public interest is served in such a way as to over-ride the private interest of the Registrant or any duty on Registrars to secure personal data. This is consistent with the typical exceptions provided by data privacy laws across the globe. (In the group’s debate there were occasional alternate views expressed by individuals who would prefer these exceptions did not exist. The consensus of the group was to recognise both the existence and the need for such exceptions.)

Proportionality of the cost of change

The OPOC proposal requires a change in the way certain data would be collected, displayed and accessed. It was understood that such changes have cost implications in their implementation. The cost implications need to be proportionate to the benefits of any proposed change.

SECTION 2 – WHAT IS THE OPERATIONAL POINT OF CONTACT (OPOC)?

2.1 Who may be an OPOC?

There may be up to two OPOCs.

AGREED:

An OPOC must be one of the following:

- the Registrant
- the Registrar
- any third party appointed by the Registrant.

2.2 How does the OPOC relate to the Registrant?

AGREED:

Where the OPOC is not the registrant, the OPOC should in broad terms have a similar relationship to the registrant as an agent. (See also below for OPOC / Registrar relationships)

2.3 Is there a need for some form of verification of the OPOC?

The objective of the OPOC is to provide a certain point of contact in the absence of the Registrant. This certainty implies a need for some form of verification and is consistent with an objective of data Accuracy within WHOIS services.

Modalities of verification:

a) Accreditation by ICANN.

This option (a system parallel to Registrar accreditation) was generally thought to be neither scaleable not practical. It assumes a small set of OPOCs and is thus not consistent with the concept of an agent relationship.

b) Verification of an active OPOC e-mail address at time of registration.

AGREED*:

- Verification of an active e-mail address at the time of registration must be obtained by the Registrar. It would be up to each Registrar to implement this in any way they choose.
- Name registration may be completed before verification of the OPOC active e-mail address.
- In order to enhance certainty and accuracy, verification of an OPOC’s active e-mail address at the time of registration must be obtained before enabling a web site to resolve based on the registered name.
- Failure to obtain that verification in a given time period must result in a failure of the registration.

* One Registrar opposed the need for verification believing the implementation to be overly burdensome. Other Registrars believed implementation would be consistent with existing practise.

Implementation options:

- 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.

2.4 Consent to be an OPOC

Is it necessary to have the OPOC (as agent for the Registrant) to give consent to be the OPOC ?

AGREED*:

- Given the OPOC acts as the agent for the Registrant and has certain obligations, the OPOC must consent to being an OPOC.
- The Registrar must obtain that consent.

- Name registration may be completed before consent is obtained.
- In order to prevent fraud, consent must be obtained before enabling a web site to resolve based on the registered name.
- Failure to obtain that consent in a given time period must result in a failure of the registration.

* One Registrar opposed the need for consent believing the implementation to be overly burdensome. Other Registrars believed implementation would be consistent with existing practise.

.

Implementation options:

- Consent may be done by requiring a consenting reply to an auto-generated e-mail (via e-mail or a web-based agree system) and obtained at the same time as verification of the OPOC e-mail address.
- The name may be put on hold status by the Registrar pending OPOC acknowledgement and then put on active status.

2.5 Proxy Services

Certain registrars offer a "proxy" service, to provide privacy protection for the Registrant. In this case the proxy is a proxy for the Registrant. From the ICANN point of view, the "proxy" is the Registered Name Holder. The proxy holds all the legal responsibilities of the Registered Name Holder in the agreement between the Registrar and the Registered Name Holder, as well as those described in the Registrar Accreditation Agreement (RAA). Registrars also further define terms and conditions of this service. The RAA provision relevant to proxy services is clause 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 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."*

The proxy service is thus essentially irrelevant to the existence of an OPOC.

AGREED:

In order to avoid a third layer between the underlying Registrant and the OPOC, where a proxy service exists, the proxy and the first designated OPOC must be one and the same.

2.6 OPOC and the tech/admin contacts

AGREED

Simplification must be an objective should the OPOC proposal move forward.

While certain Registrars and large users claim that the admin and/or tech contacts will continue to be useful even after an the addition of one or more OPOCs, other Registrars and most users prefer a merging of roles. This support for merging is conditional upon a presumption that no useful means of contact would be lost.

a) The technical contact.

There is a functional distinction between the technical contact and the OPOC

AGREED:

- The technical contact should continue to be collected and displayed when the Registrant contact details are displayed.
- When the Registrant contact details are not displayed, then the technical contact details will also not be displayed.

b) The administration contact.

AGREED

- The role of the admin contact is currently poorly understood.
- There seems to be no over-riding reason for the future collection / display of both admin and OPOC.

Implementation options:

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

SECTION 3 – THE ROLE AND RESPONSIBILITIES OF THE OPOC

Three distinct roles for the OPOC were discussed:

- RELAY
- REVEAL
- REMEDY

3.1 RELAY

The first role of an OPOC is to RELAY information from a Requestor to the Registrant. It was recognised that the introduction of the OPOC system would introduce delays for Requesters, compared to the status quo, in communicating with and/or identifying the Registrant . Therefore there is a need to specify timely deadlines for actions by the OPOC.

AGREED:

- The OPOC must have current contact information of the Registrant.
- The OPOC must RELAY an information request to the Registrant in a timely manner.
- The OPOC must meet certain implementation requirements for relaying messages from the Requester to the Registrant.

Implementation options:

These implementation requirements may include the following:

- 24x7 responsiveness
- automatic real-time forwarding of e-mail requests from Requester to Registrant
- automatic real-time forwarding of responses from Registrant to Requester
- capability to forward requests and responses in other formats (e.g. fax or post)

Timing:

- Immediate in all cases for first leg of RELAY (OPOC to Registrant). This may be automated in the case of e-mail requests.
- E-mail responses from Registrant to OPOC may also be forwarded to Requester immediately.

The group discussed what would be the typical nature of such requests. It was recognised there may be simple administrative good faith reasons and reasons relating to bad faith. In the case of bad faith the group formed a working definition of a legal request:

> “any communication that is made for the purpose of alleging a wrongful registration or use of the domain name, or wrongful activity by the registrant. Examples of such wrongful registration, use or activities include phishing, pharming, cyber-squatting, copyright and trademark infringement, and other illegal or fraudulent activities. Such a legal notice should be accompanied by reasonable evidence of the wrongful registration, use or activity.”
>
> This is compatible with the RAA. In general, this action should be taken whenever the request presents “reasonable evidence of actionable harm” (cf. the current RAA, section 3.7.7.3).
>
> It is further possible that Registrant’s might declare themselves as natural persons to avoid having a full data set published in the Whois database. If the Registrant falsely described itself as a natural person, then this may also be grounds for RELAY, REVEAL or REMEDY.

Implementation options:

- In making a request, the Requestor may complete a checklist to inform the OPOC the nature of the request. Such a checklist might have the following form:
- Reason for Request (check one)
- Alleged fraudulent activity
- Alleged intellectual property infringement
- Alleged false declaration as a natural person
- Alleged inaccurate WHOIS data
- Other (eg good faith) (please specify)

3.2 REVEAL

The second role of an OPOC is to REVEAL the unpublished contact information of the Registrant to the Requester in certain circumstances. There was discussion as to whether REVEAL duplicates the Access function described later. The Access function does NOT involve the OPOC but uniquely the Accessor and the Registrar.

AGREED

In defence of retaining both functions the following was agreed:

- Requestors may need to know the identity of the Registrant in order to serve legal notice
- Registrars inform that there is a significant cost issue if all requests go via the Registrar.
- Registrars inform that there is a scalability issue if all requests go via the Registrar.
- There is a concern that if the Access function were to be subject to an authentication mechanism, then REVEAL may be needed in particular for the pursuit of criminal activity.

ALTERNATE VIEW

There was a minority view that REVEAL is duplication of the Access function.

AGREED:

REVEAL must take place when there is ONE OF:

- “reasonable evidence of actionable harm” such as alleged fraudulent activity, alleged intellectual property infringement or false declaration as to being a natural person.
- OR alleged inaccurate WHOIS data
- OR when RELAY had failed after a specified time period.

The REVEAL must be timely.

Implementation options:

- If no Registrant response is promptly received (12 hours in the case of an e-mail request that has been forwarded by e-mail), the OPOC may retry using all available means of contacting the Registrant (e.g. telephone).
- If no Registrant response is received within 3 days (72 hours), the OPOC may be obligated to REVEAL the Registrant contact data immediately to the Requestor.

3.3 REMEDY

The third role for the OPOC discussed was that of REMEDY.

AGREED:

- Because the OPOC would be either the Registrant or an agent for the Registrant, typically it would be inappropriate for the OPOC to be the actor for any REMEDY .
- There should be exceptional circumstances where the OPOC would be an actor for REMEDY when the web site is a large host site and the Request made is to remove specific pages from the site placed there by a third party. In these circumstances the OPOC would be acting in the interests of the Registrant.
- In these exceptional circumstances REMEDY must be timely.

Implementation options

- A time line such as 24 hours may be adopted universally

SECTION 4 – COMPLIANCE AND ENFORCEMENT

This section outlines the foreseen compliance and enforcement aspects of a modified WHOIS and in particular addresses issues when the OPOC does not fulfil the designated role and responsibilities.

AGREED:

When there has been a failure of action or time-limit by the OPOC to fulfill a RELAY, REVEAL or REMEDY request, the Requestor may contact the Registrar and request one or more of the following:

- REVEAL of the Registrant's full WHOIS data.
- Immediate suspension of the name records for the subject domain and suspend web host services.
- Immediate suspension of website DNS.
- Immediate locking of the registered domain so that it cannot be transferred for a set period.

Implementation options:

- 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.

SECTION 5 – TYPE OF REGISTRANT AND DISPLAY IMPLICATIONS

5.1 Universality of OPOC

AGREED:

- After some debate it was acknowledged that from an implementation perspective, it would make sense for all Registrants (both legal and natural persons) to appoint an OPOC.

5.2 Distinction between natural and legal persons

Working definition:

- a natural person is a real living individual.
- a legal person is a company, business, partnerships, non-profit entity, association etc.

This distinction is operational in the sense that it speaks to an historical fact about the Registrant before the act of registration. It will not vary much between jurisdictions, though forms of legal persons may display such variation.

AGREED[1]

- A distinction between legal and natural persons should be made.
- This distinction must be made by the Registrant at the moment of registration.
- There is no need for validation or a challenge mechanism to this self-declaration at the moment of registration.

[1] Agreed and confirmed by WG, 14 June, 2007

AGREED[2]*:*

The implication of this declaration is that the public display of WHOIS records will be different in the following way:

Legal person	Full display of all WHOIS records
Natural person	Limited display of WHOIS records

See annex 1 for examples.

[2] Agreed and confirmed by WG, 14 June, 2007

SECTION 6 – ACCESS TO UNDISPLAYED DATA RECORDS

Today full WHOIS data records are available to any Requestor either via web-access or bulk access of the entire database. In a post OPOC world the full data records of certain Registrants will not be available by these means. This section first discusses types of access to these un-displayed records and then discusses to whom such access may be made available.

There are broadly four types of access:

- 6.1 Access to the displayed WHOIS records
- 6.2 One-time access to one specified full data record that is un-displayed
- 6.3 Regular access to numerous data records that are un-displayed
- 6.4 Bulk access to the entire database of data records that are both displayed and un-displayed in a form that all are displayed.

This situation is a consequence of the OPOC proposal. It is understood that such access does NOT involve the OPOC in any way but only concerns the relationship between the party wanting access and the Registrar. (For this reason while the language Requestor is used in other sections for a Request initially made of the OPOC, the term Accessor is used here for clarity).

The objective of Access is to enable activities in pursuit of the prevention of criminal or civil harm. In this pursuit the group recognised the exceptions in data privacy laws which allow the public interest to be served in such a way to over-ride the private interest of the Registrant or any duty on Registrars to secure personal data.

6.1 Access to the displayed WHOIS records

AGREED:

- This access (web-based or bulk) should continue in its present form and would result in access to the full data records for legal persons and the limited data records for natural persons.

6.2 One-time access to one specified full data record that is un-displayed

Access is limited to the record of a Registrant at a specific time, wherein a specific request is made to the Registrar for each incident. (This type of access cannot currently be provided via Port 43).

- This access would take place when there is “reasonable evidence of actionable harm” such as suspected fraudulent activity, suspected intellectual property infringement or suspected false declaration as to being a natural person.
- The access must be timely.

6.3 Regular access to numerous data records that are un-displayed

This access is query-based to any domain, but may come with restrictions or record-keeping obligations.

Implementation options:

- 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 made either by the Registrar or the Accessor
- there may be means to sanction Accessors for abuse of restrictions or record-keeping obligations.

6.4 Bulk access to displayed and un-displayed records

This is access to the entire database of data records that are both displayed and un-displayed in a form that all are displayed. Such access would be via Port 43 but a means of displaying the un-displayed records would be needed.

Implementation options:

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

6.5 Is there any need for Access?

The group identified two broad categories of Accessors who might have a need for such access as described above.

- Public law enforcement agencies (LEAs): governmental agencies legally mandated to investigate and/or prosecute illegal activity.
- Private actors: organisations or individuals that are not part of a LEA.

AGREED

There were circumstances where both LEAs and private actors must have access described above (6.2, 6.3, 6.4). These circumstances include suspected terrorist, fraudulent or other illegal activity, suspected consumer harm and suspected intellectual property infringement.

(An alternate view was that private actors should be denied bulk access described under 6.4 in all circumstances.)

6.6 Do those needing access require authentication?

There was discussion about the need for Registrars to authenticate in some way those parties requesting such access. It was recognised that authentication would both potentially introduce delays in Access and impose cost upon Registrars and Accessors. Among the private actors it was recognised the banking sector had especially urgent needs to address consumer fraud from acts such as phishing (identity theft).

AGREED:

It was agreed that broadly there are two mechanisms for means of access:

- Self-declaration by the Accessor (possibly backed-up by a challenge procedure by the Registrar).
- Authentication of the Accessor by a third party.

The following options were discussed and rejected as either impractical or not legally permissible on a sufficiently wide global scale:

- use of Interpol to authenticate LEAs.
- use of LEAs to authenticate the private sector.

There was no practical suggestion about how the second option (authentication) may take place in a way that was scaleable globally and proportionate to cost.

A consultant’s report considering the practicalities of an authentication mechanism for LEA’s in the United States concluded: “I am not confident that there is an organization that can properly accredit law enforcement agencies in the United States, let alone internationally”.

AGREED:

In the absence of a practical method of authentication the group recommends access be granted to LEAs and private agencies based on self-declaration by the Accessor.

Implementation options

- Self-declaration could be subject to a challenge procedure by the Registrar.

SECTION 7 – RECORD OF DISCUSSIONS AND ALTERNATE VIEWS

To be completed

7.1 Distinction between Commercial and Non-Commercial

This distinction is problematic as it relates to the future intent of the Registrant and is not coincident with the moment of Registration.

If this distinction were to be made, it could be made as a self-declaration at the point of registration. If this distinction were to be made, *natural persons* could be considered engaging in commercial activities if one of the following indicative criteria is satisfied:

- The offer or sale of goods or services
- The solicitation or collection of money or payments-in-kind
- Marketing activities, advertising, paid hypertext links
- Activities carried out on behalf of legal persons
- Certain types of data processing.

Overall the group felt that the distinction between commercial and non-commercial activities is not by itself sufficiently timely at the point of registration nor easily operational. A set of strict, subordinate criteria might make it operational. Working group members are invited to elaborate.

ANNEX 1 – WHOIS DATA DISPLAY OPTIONS

Record	**WHOIS today**	**Limited (OPOC)**	**Full (OPOC)**
Domain ID:	x	x	x
Domain Name:	x	x	x
Created On:	x	x	x
Last Updated	x	x	x
Expiration Date:	x	x	x
Sponsoring Registrar:	x	x	x
Status*:	x	x	x
Registrant ID:	x	x	x
Registrant Name:	x	x	x
Registrant Organization:	x	x	x
Registrant Street1:	x		x
Registrant Street2:	x		x
Registrant Street3:	x		x
Registrant City:	x		x
Registrant State/Province:	x	x	x
Registrant Postal Code:	x		x
Registrant Country:	x	x	x
Registrant Phone:	x		x
Registrant Phone Ext.:	x		x
Registrant FAX:	x		x
Registrant FAX Ext.:	x		x
Registrant Email:	x		x
Natural person#		x	x
Legal person#		x	x
Proxy service operating#		x	x

Record	WHOIS today	Limited (OPOC)	Full (OPOC)
OPOC*# ID:		x	x
OPOC Name:		x	x
OPOC Organization:		x	x
OPOC Street1:		x	x
OPOC Street2:		x	x
OPOC Street3:		x	x
OPOC City:		x	x
OPOC State/Province:		x	x
OPOC Postal Code:		x	x
OPOC Country:		x	x
OPOC Phone:		x	x
OPOC Phone Ext.:		x	x
OPOC FAX:		x	x
OPOC FAX Ext.:		x	x
OPOC Email:		x	x
Admin ID:	x	?	?
Admin Name:	x	?	?
Admin Organization:	x	?	?
Admin Street1:	x	?	?
Admin Street2:	x	?	?
Admin Street3:	x	?	?
Admin City:	x	?	?
Admin State/Province:	x	?	?
Admin Postal Code:	x	?	?
Admin Country:	x	?	?
Admin Phone:	x	?	?
Admin Phone Ext.:	x	?	?
Admin FAX:	x	?	?

Record	**WHOIS**	**Limited**	**Full**
	today	**(OPOC)**	**(OPOC)**
Admin FAX Ext.:	x	?	?
Admin Email:	x	?	?
Tech ID:	x		x
Tech Name:	x		x
Tech Organization:	x		x
Tech Street1:	x		x
Tech Street2:	x		x
Tech Street3:	x		x
Tech City:	x		x
Tech State/Province:	x		x
Tech Postal Code:	x		x
Tech Country:	x		x
Tech Phone:	x		x
Tech Phone Ext.:	x		x
Tech FAX:	x		x
Tech FAX Ext.:	x		x
Tech Email:	x		x
Name Server*:	x	x	x

Key:

*	multiple entries possible
x	data collected and displayed
	data collected but not displayed
░	data not collected
▨	merged data with OPOC
#	new data element conditional on new policy

ANNEX 2 – GLOSSARY

Accuracy:

Existing provisions in the Registrar Accreditation Agreement on Whois Data Accuracy.

ICANN's contracts with accredited registrars require registrars to obtain contact information from registrants, to provide it publicly by a Whois service, and to investigate and correct any reported inaccuracies in contact information for names they sponsor.

The following provision of the ICANN Registrar Accreditation Agreement (RAA) <http://www.icann.org/registrars/ra-agreement-17may01.htm> is relevant to the accuracy of registrar Whois data:

> *3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions:*
> *3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.*
> *3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.*