Draft Outcomes Report of the Whois Working Group

STATUS OF THIS DOCUMENT

This is Version 1.6 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 a gathering of positive opinion, but a range of alternative views exist and broad agreement has not been reached;
- **Alternative views** – differing opinions that have been expressed, without garnering enough following within the WG to merit the notion of either Support or Agreed.

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. It should be noted that in the context of this large group (60 plus) most of whom only ever spoke in an individual capacity this determination was challenging.

SECTION 1 OBJECTIVE

The public interest: balancing privacy and harm

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 other public interest goals of consumer fraud and acts of bad faith by certain Registrants.

The essence of the underlying debate was to mirror existing legal exceptions when it is necessary to enable activities in pursuit of the prevention of harm that may be prevented by criminal, civil or administrative procedures. In this pursuit it is understood that there are exceptions to data privacy laws when the public interest is also served in such a way as to over-ride any private interest of the Registrant or any duty on Registrars to keep personal data secure. The group was keen to be consistent with the typical exceptions provided by data privacy laws across the globe.

This objective would seem to be consistent with the WHOIS principles of ICANN's Government Advisory Committee (GAC). The group has taken note of those principles, which were advanced with the intention of providing guidance to the policy process.

(In the group's debate there were occasional alternative views expressed by individuals who would prefer the exceptions in national laws did not exist. The consensus of the group was to recognise both the existence and the need for such exceptions.)

Balance or harmony?

For many users there was little conflict between the two goals (protection of privacy and protection from crime). These users expressed a concern about misuse of personal data primarily when that data would fall into the hands of criminals. In other words data privacy for these users was a strategy with the same objective (protection from crime).

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 and to the ability of those who bear the costs. There was discussion as to where these costs should fall. Outcomes of those discussions appear in the relevant section and are also one of the subjects of section 8 (calls for further study).

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:

- The OPOC should have a consensual relationship to the Registrant with defined responsibilities.
- There will need to be a change to both the Registrar Accreditation Agreement (RAA) and subsequently Registrar-Registrant's agreements to reflect this relationship.

ALTERNATIVE VIEWS:

There was one view that the OPOC need merely be a designee with no indication of consent.

Implementation: It is not intended that the implementation of this need bind any party to any formal legal obligations that may exist in national law.

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 the existing obligation for data Accuracy within WHOIS services.

SUPPORT:

- 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.
- Once verification is obtained, web-site resolution must be rapid.

ALTERNATIVE VIEWS:

Two registrar members opposed the need for verification believing the implementation to be overly burdensome.

One registrar member believed implementation would be consistent with existing practise.

One registrar member commented that anyway the existing registration process with certain registries takes weeks.

One user view was to not even enable registration until verification was complete.

185 One user view was that verification was unnecessary because that user opposed
186 the concept of the OPOC having defined responsibilities.
187 One Registry member disagreed with the recommendation.
188

189 Implementation options:
190 ▪ Verification could be done by requiring a reply to an auto-generated e-mail.
191 ▪ Verification may be obtained at the same time as consent (see below)
192 ▪ The name may be put on hold status by the Registrar pending verification
193 and then put on active status.
194 ▪ Registrars may engage with Registries with respect to hold status.

195

2.4 Consent to be an OPOC

Is it necessary to have the OPOC to give consent to be the OPOC ?

AGREED:

Ultimately, it is the Registrant who is responsible for having a functional OPOC in the way described below.

SUPPORT:

- Given the OPOC should have a consensual relationship to the Registrant with defined responsibilities, the OPOC must consent to being an OPOC.
- 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.
- Once consent is obtained, web-site resolution must be rapid.

ALTERNATIVE VIEWS:

Two registrars members opposed the need for consent believing the implementation to be overly burdensome.

One registrar member believed implementation would be consistent with existing practise.

One registrar member commented that anyway the existing registration process with certain registries takes weeks.

One user view was that verification was unnecessary because that user opposed the concept of the OPOC having defined responsibilities.

One registry member disagreed with the recommendation.

Who should obtain consent?

SUPPORT:

The Registrar must obtain consent.

ALTERNATIVE VIEWS:

One registrar member said that it may be possible for the Registrant to obtain consent and during registration confirm to the Registrar that consent had been obtained.

One user commented that this alternative view would be burdensome on Registrants and posed challenges in tracing responsibility.

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.
- Registrars may engage with Registries with respect to hold status.
- Registrars may need to consider changes to billing functions.
- If more practical, the responsibility for “the process of consent” could lie with the Registrant and be regulated within the Registrar-Registrant agreement.

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.

ALTERNATIVE VIEWS:

One registrar member saw no need for any restriction.

One user believed that a third layer was good for data privacy.

2.6 OPOC and the tech/admin contacts

AGREED

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

While one Registrar and one large user claimed 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. (The support from users for merging is conditional upon a presumption that no useful means of contact would be lost).

a) The technical contact.

There is an intuitive functional distinction between the technical contact and the OPOC although regrettably there is no formal definition of the role of the technical contact.

AGREED:

- The technical contact should continue to be 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 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 Requester 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)

Implementation options on 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 good faith reasons and reasons relating to bad faith. In the case of bad faith the group considered the likely rationale for a 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 notice would be accompanied by reasonable evidence of the wrongful act.

It is possible that Registrants might declare themselves as natural persons to avoid having a full data set published in the WHOIS database.

It was recognised that a clear definition was required for implementation. The intent here is to be compatible with the RAA and its reference to: "reasonable evidence of actionable harm" (cf. the current RAA, section 3.7.7.3). Hence, the following phrasing is used in the report to capture this idea:

> "reasonable evidence of actionable harm" such as suspected fraudulent activity, intellectual property infringement, suspected false declaration as to being a natural person, or where other criminal, civil or administrative laws may be infringed".

Implementation options:

- In making a request, the Requester may complete a checklist to inform the OPOC the nature of the request. Such a checklist might have the following form: Reason for Request is 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 eg good faith (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:

- Requesters may need to know the contact information of the Registrant in order to serve legal notice.
- If a Registrant had originally provided inaccurate data, then direct Access to the Registrar would be useless. It may be only the OPOC would have accurate contact information for the Registrant.
- 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 VIEWS:

There was one user view that REVEAL is duplication of the Access function.
There was one user view that REVEAL might contravene a national law.
There was one view in favour of authentication of the Requester.
There was one view in favour of a due legal process before an unwilling REVEAL.

AGREED:

REVEAL must take place when there is ONE OF the following conditions:

- "reasonable evidence of actionable harm" suspected fraudulent activity, suspected intellectual property infringement, suspected false declaration as to being a natural person, or where other criminal, civil or administrative laws may be infringed.
- OR reasonable evidence of inaccurate WHOIS data
- OR when RELAY had failed after a specified time period.

The REVEAL must be timely.

ALTERNATIVE VIEWS:

One view was that inaccurate WHOIS data should not be a condition.

One view was that failure of RELAY should not be a condition.

One view was that the RELAY test should be cumulative (an "AND" option).

One registry member disagreed with the recommendation.

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 Requester.
- Reasonable evidence needs to be defined.

3.3 REMEDY

The third role for the OPOC discussed was that of REMEDY. It was recognised that this is a narrow role under certain specific conditions.

AGREED:

- Because the OPOC would be either the Registrant or in a consensual relationship with the Registrant, it would be inappropriate for the OPOC to be the actor for a REMEDY that may not be in the interests of the Registrant or for which the Registrant does not consent.
- The OPOC should be the actor for REMEDY when the Registrant consents. Such a case may be when a 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 circumstances REMEDY must be timely.

Note: The group recognised that this exceptional REMEDY function was technically outside of the scope of the group's task as it relates to an OPOC interaction with the hosting Internet Service Provider (ISP). Nevertheless, it is worth recording here as it is a role of the OPOC.

ALTERNATIVE VIEWS:

One registrar member disagreed with the recommendation.

One registry member disagreed with the recommendation.

Implementation options

- Implementation is required outside of the scope of WHOIS services.
- Timely should be interpreted as a time line that is proportionate to the harm.

SECTION 4 – COMPLIANCE AND ENFORCEMENT

This section outlines the foreseen compliance and enforcement aspects of the OPOC proposal and addresses issues when the OPOC does not fulfil the designated role and responsibilities. Thus a Registrar obligation occurs uniquely when there is a failure of the OPOC to RELAY, REVEAL or REMEDY as described above.

AGREED:

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

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

AGREED

In contrast to the Access function (described later) it was generally felt that this service should be free of cost to the Requester as it relates to a failure of the OPOC to perform. Thus any additional costs for this service would be factored into the fees charged by Registrars to all Registrants.

ALTERNATIVE VIEWS:

One registrar felt that actions related to web-site suspension were out of scope.

One view was that actions related to web-site suspension should be the only ones in scope.

One registrar member felt that all services should be chargeable.

One registrar member disagreed with the recommendation.

One registry member disagreed with the recommendation.

One LEA member wanted a means to regulate or sanction OPOCs who consistently failed to perform.

Implementation options:

- 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.

SECTION 5 – TYPE OF REGISTRANT AND DISPLAY IMPLICATIONS

5.1 Universality of OPOC

AGREED:

- 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:

- A distinction between legal and natural persons must 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 so long as a post registration mechanism exists.

AGREED*:*

The implication of this declaration is that the public display of WHOIS records must 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.

ALTERNATIVE VIEWS:

One registrar member disagreed with the recommendation.

One registry member disagreed with the recommendation.

Implementation options:

For clarity, because in some countries a natural person may also be a sole trader (and thus a legal person), a checkbox (to select natural or legal) as part of the registration process may be required.

SECTION 6 – ACCESS TO UNDISPLAYED DATA RECORDS

Today full WHOIS data records are typically available to any Requester either via web-access or bulk access of the entire database. In a post OPOC world it is proposed that the full data records of certain Registrants (natural persons) 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. 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 Requester 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 legitimate pursuit of the prevention of harm that may be prevented by criminal, civil or administrative procedures. In this pursuit the group recognised the exceptions to data privacy laws which, in certain circumstances, override the duty on Registrars to secure personal data.

6.1 Access to the displayed WHOIS records

AGREED:

This access 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.

The group discussed three additional types of access. The sub-sections that follow (6.2, 6.3, 6.4). are descriptions not policy recommendations.

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

This type of access would be limited to the record of a Registrant at a specific time, wherein a specific request is made to the Registrar for each incident.

- This access would take place when there is “reasonable evidence of actionable harm” such as suspected fraudulent activity, suspected intellectual property infringement, suspected false declaration as to being a natural person, or where other criminal, civil or administrative laws may be infringed.
- Such access would need to be timely to be effective. (Timeliness would be defined as proportionate to the suspected harm and related to the means of access).

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

This type of access would be query-based to any domain. Access would take place when there is “reasonable evidence of actionable harm.”

Implementation options:

- A pre-registration system by Registrars for 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 restrictions.

6.4 Bulk access to displayed and un-displayed records

This type of access would be access to the entire database of data records that are both displayed and un-displayed in a form that all are displayed. 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 an LEA.

AGREED

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

SUPPORT:

- There were circumstances where private actors may need access described above (under 6.4).

ALTERNATIVE VIEWS:

There were some views that private actors should be denied access described under 6.4.

One registrar member disagreed with the recommendation.

One registry member disagreed with the recommendation.

Implementation options:
The “circumstances” for allowable Access need to be consistently defined.

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 (probably 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 known method about how authentication of an Accessor by a third party may take place in a way that was scaleable globally and proportionate to cost. Additionally, some LEAs reported fundamental challenges to the concept of private sector authentication of public sector entities: this would seem to reverse the usual role of government. A US consultant's report considering the practicalities of an authentication mechanism for LEAs in the United States discussed possible means but in summary 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:

- The feasibility, practicality and cost-effectiveness of authentication mechanisms for LEAs and private actors should be an area for further study (see section 8).

AGREED:

- In the absence of a known method of authentication today the group recommends access be granted to LEAs and private agencies based on self-declaration by the Accessor.
- A system of safeguards to prevent abuse of this Access is needed such as a challenge mechanism by Registrars.

ALTERNATIVE VIEWS:

Certain user members believed self-declaration was insufficient and that authentication was essential: thus OPOC implementation should wait until authentication systems existed.

One registrar member disagreed with the recommendation.

One registry member disagreed with the recommendation.

Implementation options

- A concise description of the grounds for requiring Access is needed.
- Private actors may enter into prior agreements with a Registrar to enable or speed Access.
- For self-declaration to be subject to an effective challenge procedure by the Registrar, work is needed to determine “effective”.

6.7 Should any Access services be chargeable?

There was discussion as to whether any of the Access options described above in 6.2, 6.3 and 6.4 should be chargeable by Registrars to those requiring Access. Reasons in favour were:

- to recover costs
- to impose costs on those requiring the service
- to deter abuse that may arise in a free system
- to assist with monitoring.

Reasons against were:

- a concern that fees may be excessive to Accessors
- a concern that fees may go beyond nominal or cost recovery and become profit-generating
- a concern that there was additional (wasted) cost in merely setting up a new fee collection system.

AGREED

There should be no assumption that Access services would be entirely free of cost to Accessors.

ALTERNATIVE VIEWS:

One user view was that all costs should be factored into the basic user fees charged by Registrars thus avoiding the need and cost of additional mechanisms.

Implementation options:
Registrars may consider charging a nominal fee for Access services.

SECTION 7 – RECORD OF DISCUSSIONS OF OTHER OPTIONS

This section records issues, not mentioned elsewhere in the report, where there was substantial discussion and lists those options that did not achieve general support.

7.1 OPOC accreditation by ICANN

(See section 2). The group discussed two means of accreditation of the OPOC. A formal system of accreditation by ICANN and a system of verification and consent. The more formal option of a system of centralised accreditation by ICANN (a system parallel to Registrar accreditation) was generally thought to be neither scaleable not practical. It assumed a small set of OPOCs and is thus not consistent with the concept of a set of widespread consensual relationships.

7.2 Distinction between Commercial and Non-Commercial Registrants

(See section 5). 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.

SECTION 8 – FEASIBILITY STUDIES

Throughout the group's time there have been a number of issues that were unresolved as a result of technical or legal uncertainty. Such issues lend themselves to short focused studies to assess feasibility and certainty.

These issues include:

- an assessment and comparison of the incremental costs of OPOC implementation versus the benefits anticipated. Within this are subsets of cost-related studies:
    - the costs to implement the verification and consent proposals described in sections 2.4 and 2.5;
    - the costs to implement the Request/compliance issues of section 4;
    - the costs to implement the Access options described in section 6;
    - the marginal cost of a system to implement a new fee-based system for Accessors compared with recovering additional costs from user fees using existing systems;
- data privacy issues arising from the self-declaration of Accessors proposal described in section 6;
- mechanisms for a practical, cost-effective, globally scaleable means of authenticating Accessors as described in section 6.

785 ANNEX 1 – WHOIS DATA DISPLAY OPTIONS

786

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 today**	**Limited (OPOC)**	**Full (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

787 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

788

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.*