1. INTRODUCTION

1.1 Previous Discussion

WHOIS has been a topic of interest and focus for ICANN since its early days. ICANN's DNSO (Domain Name Supporting Organization, the precursor to the gNSO) created a Names Council Task Force to first consider WHOIS. Based on the recommendations of that Task Force, the DNSO created a policy Task Force, with the terms of reference: "Consult with the community with regard to establish whether a revision is due, and how best to address"; this Task Force, composed of representatives from all constituencies, including the ccTLDs and the General Assembly, launched a survey of WHOIS and its use. The Task Force undertook the survey and analysis of the responses, and prepared a report that included both consensus policy recommendations and other considerations for the Council to consider in further policy work. The survey consisted of 20 questions, 19 of which are multiple choice, with narrative response allowed, and one question that was free form and allowed respondents to provide any additional input they chose. In order to ensure road and diverse consideration of the survey's findings, the Task Force was expanded to include up to three representatives of each of the constituencies of the then DNSO, and the General Assembly. The survey finding and analysis, and membership from the Constituencies, General assembly can be found at {insert link}

In order to meet its mandate of consulting broadly with the community, in addition to the survey and analysis of the responses, the Task Force undertook extensive outreach to various experts and groups, in order to inform and provide critical additional input to the Task Force, including consultation within the constituencies and General Assembly. Consultation via conference calls were held with experts from ccTLDs, IETF leadership, the Security and Stability Advisory Committee regarding its report on the impact of WHOIS on security and stability of the Internet; two presentations were hosted with. Name and the IETF CRISP working group. Transcripts of these conference call consultations were provided and are available in the DNSO archive. In the course of the work of the Task Force, workshops were also held to brief Council, the Board and the community; these workshops included both reports on the work of the Task Force and its findings, and also on the expert input the Task Force was receiving, including questions related to privacy and accuracy of data.

A final policy report [November 30,2002] was prepared, with public comment period, and a final Policy Report published on December, 2002, proposing both consensus policy an d enhancement s in ICANN's enforcement of existing obligations in two areas: Accuracy and Bulk access. Further work was recommended for both areas and on searchability and consistency of data elements across all TLDS. At its Amsterdam meeting, the Council discussed the TF report and reopened the report for further comment by constituencies and the community. And, at this meeting, the Council also established an Implementation Committee, with a deadline of January 31,2003.

Certain elements of Accuracy of WHOIS data were recommended as consensus elements as established by the initial WHOIS Task Force. The consensus policy recommended by the TF, would require the notification, at least annually, of a reminder to the registrant, that their data must be accurate, or that they can potentially lose their registration. Further consensus recommendations included how to deal with names that are deleted due to inaccurate data and reinstatement opportunities [dependent upon a standard deletes policy that was subsequently developed and approved by Council]. . These became consensus policy of ICANN, based on the Council's approval, and Board acceptance of the recommendation of consensus policy.

A second consensus policy recommendation related to bulk access to WHOIS data was presented: Use of bulk access WHOIS data for marketing should not be permitted. The TF recommended modifications, as needed in registrars access agreements to prevent third parties from using the data for marketing purposes, regardless of the media used. This was forwarded to the Board as consensus policy.

. The recommendations of the WHOIS Task Force included the continuance of work by Council in several areas {link:]. These were not presented as consensus policy but as recommendations to Council for consideration in the further work of Council related to WHOIS.

Documents of relevance include the final consensus policy recommendations [Final Report of the GNSO Councils WHOIS TF on Accuracy and Bulk Access, Feb. 6, 2003] approved by the Council, and forwarded to the ICANN Board on (insert date). The report of the Task Force also included some recommendations to Council that were recommendations to ICANN staff. These recommendations are also contained in the final report approved by Council. (Insert link).

The Implementation Committee report can e found at {link]. The Council received the Implementation Committee report and included its recommendations in the final Report forwarded to the Board (insert date).

1.2 Genesis of the Task Force

Following the work and recommendation of the original TF on WHOIS, council discussed how to proceed on WHOIS issues. . Council did not consider the previous TF further recommendations definitive, and thus, there may appear to be something of a discontinuity between the recommendations for further work provided by the initial WHOIS TF and the existing Council TF work on WHOIS. Some areas suggested by the previous TF are being addressed, and some are pending.

The Council was divided on how to proceed in addressing next stages of work on WHOIS, with some members preferring to focus on the recommendations from the Task Force for next stages of work, and others primarily concerned about privacy aspects of WHOIS. Council decided to create a WHOIS Privacy Steering Group, chaired by Bruce Tonkin, also chair of the Council, in order to examine what issues should be addressed by

Further WHOIS TFs of Council. Efforts were made to identify a neutral chair, but given Time constraints, the group agreed to conduct their work with the chair of Council as the Chair of the group. The group included members from all constituencies, liaisons from ALAC, ccTLDs, GAC and Nominating Committee members. [see list at …] The group worked to identify priorities for the community based on a review of the constituencies and the stakeholders perspectives. [See August 14.2003 WHOIS Privacy Issue Table]. This work provided the basis for Council's chartering of further Task Force work on WHOIS. The work of this group is important to guide the development of the TFs of Council, and remains a relevant document to inform and advise all the TFs, and the Council itself.

To inform its work, the Privacy Steering Group held several conference call meetings, met face to face at ICANN meetings, and hosted two workshops: Montreal and Tunisia, where invited experts from key stakeholder groups were invited to present. Presentations were invited from all constituencies and the At Large Advisory Committee. participants from the OECD, the U.S. Federal Trade Commission and the US Department of Justice; the European Commission; WIPO, and data privacy experts from Europe, and industry experts in intellectual property issues affected by WHOIS, as well as ccTLD managers who were invited as experts on how particular issues are dealt with within their ccTLD. (see {insert link} for presentations and agenda for workshops at Montreal and Tunisia).

The Council reviewed the work and recommendations of the original TF, and the WHOIS Privacy Steering Group, as well as the public comments and workshop presentations, and decided to create a new PDP related to WHOIS policy. The Council was divided on how best to address the work and after much debate, decided to launch three simultaneous TFs on WHOIS, with the assumption that the alignment of recommendations will take place in Council. The TF were launched on [date]; the Descriptions of Work (DOW) of each Task Force is available at {insert link].

1.3 Terms of Reference

The purpose of this task force is to determine:
a) What the best way is to inform registrants of what information about themselves is made publicly available when they register a domain name and what options they have to restrict access to that data and receive notification of its use?

b) What changes, if any, should be made in the data elements about registrants that must be collected at the time of registration to achieve an acceptable balance between the interests of those seeking contact-ability, and those seeking privacy protections?

c) Should domain name holders be allowed to remove certain parts of the required contact information from anonymous (public) access, and if so, what data elements can be withdrawn from public access, by which registrants, and what contractual changes (if any) are required to enable this? Should registrars be required to notify domain name holders when the withheld data is released to third parties?
If registrants have the ability to withhold data from public anonymous access, will this increase user incentive to keep the contact information they supply current and accurate.

To ensure that the task force remains focused and that its goal is achievable and within a reasonable time frame, it is necessary to be clear on what is out of scope for the task force.

Out-of-scope:

The task force should not examine the mechanisms available for anonymous public access of the data - this is the subject of a separate task force.

The task force should not examine mechanisms for law enforcement access to the data collected. This is generally subject to varying local laws, and may be the subject of a future task force.

The task force should not study new methods or policies for ensuring the accuracy of the required data, as this will be subject of a separate task force.

The task force should not consider issues regarding registrars' ability to use Whois data for their own marketing purposes, or their claims of proprietary rights to customers' personal data.

1.4 Overview of Recommendations

The task force discussions and ensuing recommendations focus on our attempt to balance the needs and rights of registrants to keep their personal information from wrongful access and misappropriation while enabling legitimate uses of the data elements and respecting the needs of those requesting access to the data.

Some changes to current Whois policy that make up the final recommendations are as follows:

- More conspicuous notice to registrants by registrars, at the point of registration, of the possible uses of Whois data.
- More conspicuous notice and clarifications to registrants by registrars, at the point of registration, as to the process by which registrant data will be shared.
- The principle of tiered access to Whois data elements is accepted, subject to reaching consensus on viability, balance of interests and financial feasibility.
- Uniform implementation of Whois policy by all registrars.
- Registrars should not have to violate local data protection laws in order to conform with Whois policy. If there is a conflict of law and Whois policy, a process should be in place to allow for registrars to show such conflict and detail the change needed for it to conform to the respective local laws.

2. FINDINGS ON EACH ISSUE

2.1 Notification and Consent

According to the ICANN Registrar Accreditation Agreement (RAA), Registrars are required to form an agreement with Registered Name Holders containing the following elements.

Section 3.7.7 of the RAA addresses the requirements of the Registrar/Registrant agreement, including the need for accurate and reliable registrant contact information. To the extent the notice to registrants of data elements collected and displayed are not clear or may be overlooked by registrants based on the overall length and complexity of the registration agreement, it is useful to change the format so that better notice is delivered to registrants. The task force finds that disclosures regarding availability and access to Whois data should be set aside from other provisions of a registration agreement by way of bigger or bolded font, a highlighted section, simplified language or otherwise made more conspicuous.

It follows that separate consent to the Whois disclosures is also useful. By obtaining separate consent from registrants, at the time of agreement, to the specific Whois data provisions, it would further draw attention to and facilitate better understanding of the registrar's Whois disclosure policy.

2.2 Proxy Registrations

"Proxy Services" were looked at during the Task Force's data analysis phase; see appendix [...] for results from that phase of the Task Force's work. Groups that submitted preliminary statements during this phase of the Task Force's work included the IPC, NCUC, ISPCP, and ALAC. ISPCP pointed to various proxy providers. IPC indicated that only little anecdotal data about how these services work in practice was available. NCUC warned that the proxy situation means that an intermediary is inserted into the contractual relationship between the "actual" registrant and the registrar, and that this party can do whatever it wants with the domain name. NCUC also pointed out that proxy services are not providing anonymity suitable to protect free speech, because of liabilities incurred by those offering these services. ALAC identified disclosure of actual registrants' identity on slight provocation as the chief problem with proxy services, and suggested that wrongdoing could be stopped without revealing actual registrants' identities. ALAC also pointed to the risks created by inserting a proxy into the contractual relationships between registrar and actual registrant.

Proxy Services were addressed in formal constituency statements by the IPC and NCUC. IPC suggested further research on the use of these services, and identified a number of issues that could be addressed in this kind of research.

NCUC specifically proposed removing sections from the Registrar Accreditation Agreement that require proxy services to disclose registrant and administrative contact data for reasons falling short of legal due process (specifically section 3.7.7.3 of the

RAA), and characterized the services as “not providing true protections for privacy or freedom of expression.”

During discussion, NCUC and ALAC representatives suggested that these proxy services do not provide sufficient privacy protections, and proposed stricter protections. IPC recommended further study of proxy services, since the evidence available on the business practices of existing proxy services was insufficient.

Registrar and ALAC representatives argued that regulating the conduct of proxy services that work by registering domain names that are then sub-licensed to registrants proper would amount to generally regulating registrant conduct, and would be undesirable.

Registrar and ALAC representatives also argued that use of this kind of proxy service as a model for large-scale privacy protection would undermine basic assumptions that are at the heart of the new inter-registrar transfers policy, and would break this policy. IPC representatives suggested that further research in this area was needed.

A registrar representative pointed out that proxy services should not be considered a final solution, and that pushing registrants to a separate for-pay service may not address local privacy law concerns. It was also noted that, when provided free of charge, proxy services would effectively lead to a tiered access proposal. A registrar representative stated that his constituency may be more comfortable with a tiered access model than with proxy services, but that no consensus has yet been reached.

Related models under which registrars proxy some communication for registrants were also discussed in the context of balancing contactability and privacy: It was, for instance, suggested that registrars may provide an electronic point of contact for registrants and domain name contacts, without making the registrant's usual e-mail address publicly available.

2.3 Local Law

Registrars are obligated per section 3.3 of the RAA to make available a predefined set of data elements on the whois. As this dataset might contain personal data and Registrars contracting with ICANN, to be able to provide domain name registration services, might operate under different legislation than ICANN the taskforce was mandated in the DOW of Taskforce 2

> *Document examples of existing local privacy laws in regard to display/transmittal of data (DOW TF2)*

to investigate if this obligation might lead to problems in regard to existing privacy laws and regulations in these legislations.

After documenting and reviewing the examples of local privacy laws it is the Taskforce finding that different nations have very different privacy laws and that the determination

whether they are applicable to the gTLD whois situation is not an easy one. The Taskforce nevertheless views it as proven that there is certainly a risk of conflict between a registrars or registries legal obligations under local privacy laws and their contractual obligations to ICANN.. They most popular example is the just recently revised .name whois policy which had to be changed to comply with a request of the UK Data Commissioner. In theTask Force's questionnaire the Global Names Registry stated that:

> *"we have changed, and may have to change in the future, the WHOIS policy to follow local regulation as it evolves and incase of successful complaints to the Information Commissioner." (http://www.gnso.icann.org/mailing lists/archives/dow2tf/msg00152.html)*

Since the variety of the existing local privacy laws does not allow for a One-Size-Fits-All solution the Registrars and Registries encountering such local difficulties should be allowed an exception from the contractual whois obligation for the part of the whois data in question by the local regulation. after proving the existence of such a regulation. In addition a procedure should be established for seeking to resolve such conflicts with local authorities as new regulations evolve in a way that promotes stability and uniformity of the Whois system.

Such steps will undoubtedly achieve a greater legal certainty and foster the international competition on the domain name market.

2.4 Collection of Data

Through the use of questionnaires to which constituencies and members of the public were invited to respond, the Task Force attempted to determine whether there was any consensus on the elimination or expansion of the existing data elements that are collected and disclosed via Whois. The responses do not indicate any such consensus. Some respondents called for a drastic reduction in the number of data elements; some respondents called for additional data elements to be collected and made available; others expressed satisfaction with the status quo. Accordingly, the Task Force proposes the following conclusions on the issues identified in Task/Milestone 2 of the Task Force 2 Description of Work:

- all of the data elements now collected are considered by at least some constituencies to be necessary for current and foreseeable needs of the community, though others dispute this;
- the Task Force deferred to Task Force 3 on the issue of whether Whois data can be acquired accurately at low cost;
- there was no consensus about whether any of the current elements should be made voluntary;
- some additional data elements were proposed, but questions were raised about whether some of these (e.g., date and method of last verification of data) fell within the purview of TF3 rather than TF 2;
- no issues were raised about how the data may be acquired in compliance with

applicable security, and stability considerations. While some view the acquisition of this data as raising privacy concerns, there was no consensus on this point, and the Task Force devoted more of its time and resources to discussing the issues raised in Tasks/Milestones 3 and 4 (limiting data made available for public access/existing and future options to maintain registrant anonymity).

2.5 Publication of Data

The topic of publication of data received considerable attention in TF2. Originally published for technical and operational purposes, the 20 year old WHOIS protocol has developed a range of secondary uses (outlined below). Once limited to the information of research and technical institutions in a small and limited network, the data -- including registrant name, address, phone and email -- originally invoked no privacy concerns, but today raises the specter of privacy and freedom of expression infringement (outlined below).

One topic the TF addressed and did not answer was the purpose of the database. Our mandate was to balance contactability and privacy, which we have tried to do. We leave to another PDP process the knotty question of the ultimate purposes of this database, and whether and how they can change.

Findings:

1. WHOIS data continues to serve a host of technical and operational functions for Registries and Registrars. Transfers and other technical processes require the ability to access, verify and transfer WHOIS data.

2. WHOIS data includes personal and sensitive data of the type that people are generally allowed to limit and control in other mediums (such as address and phone in an unlisted phone number, and the control over secondary uses given to owners of personal data in European countries and other countries with comprehensive data protection legislation). Such personal data is found in the registrant, administrative contact and technical contact fields.

3. Publication of data serves a host of secondary purposes, including combating spam, policing trademarks and copyrights, availability/offers for domain names and checking registration data of a domain name by its owner.

4. Publication of WHOIS data raises a host of privacy problems, including identity theft, telemarketing, spamming and other forms of email and telephone harassment, stalking, abuse and harassment by groups acting outside of normal scope and legal need.

5. Publication of all WHOIS data to the world for access on an anonymous basis does

not serve the balance of contactability and privacy.

6. Data requesters want timely, even immediate, responsiveness to their requests for personal/sensitive data. Data subjects (domain name holders) want timely, even immediate, notification when their personal/sensitive data is requested and revealed to a third party.

Possible Balances:

While (as of this writing) TF2 has not come to a final decision regarding which Tiered Access model to recommend, several models were submitted in Constituency statements. The Registries recommended that only General Information be provided in the WHOIS (which is technical data without registrant, administrative contact or technical contact information). The Registrars recommended a 3-tiered system with limited information in the public WHOIS (name/country of registrant, administrative contact and technical contact) and technical data; additional information at a screened-access second tier (name/address of registrant, administrative contact and technical contact) and all data displayed for technical purposes by registries and registrars.
Noncommercial Users Constituency called for publication of technical contact data in the WHOIS, but removal of all registrant and administrative contact fields. ALAC also requested removal of all personally identifying information, but asked as an alternative for notification of the domain name holder when his/her personal data was revealed.

A compromise proposal submitted to the TF called for a combination of the elements above: reduction of data available to the public for anonymous and unlimited access; additional but limited contact information provided to a party who can verify his/her/its identity and state a specific reason for the access to the particular domain name data; confirmation and then release of data via an automated process; immediate notification of the domain name holder by email of the release of personal data (allowing domain name holder to act for personal safety (e.g., data released to stalker) or enforce legal rights).

The model to emerge should take into consideration the most closely-held concerns of data users and data subjects, and those who protect their legal rights. Data users want contact data for domain name holders, especially during a pending legal investigations of a technical nature (such as spoofing or spamming). Data subjects (domain name holders) want personal/sensitive data provided only on as-needed and individual basis, and not in unlimited form to a predetermined group of data requesters. Data protection officials are concerned that overly broad reach into the data without accountability and with broad searching capabilities (e.g., wildcards) will be privacy-intrusive, disproportionate and provide a general presumption of guilt.

3. RECOMMENDATIONS

3.1 Notification and Consent

ICANN should:

(a) incorporate compliance with the notification and consent requirement (R.A.A. Secs. 3.7.7.4, 3.7.7.5) as part of its overall plan to improve registrar compliance with the RAA. (See MOU Amendment II.C.14.d).

(b) issue an advisory reminding registrars of the importance of compliance with this contractual requirement, even registrars operating primarily in countries in which local law apparently does not require registrant consent to be obtained.

(c) encourage development of best practices that will improve the effectiveness of giving notice to, and obtaining consent from, domain name registrants with regard to uses of registrant contact data, such as by requesting that GNSO commence a policy development process (or other procedure) with goal of developing such best practices.

3.2 Proxy services

The Task Force considered a proposal by the non-commercial users' constituency to strike section 3.7.7.3 of the RAA based on privacy and anonymity concerns. Concerns with proxy services were also raised with respect to issues surrounding the far-reaching control that proxy registration service providers can exercise over registrations: In the typical "proxy" setting, the service provider enters into a registration agreement and then sub-licenses the domain name to the "actual" registrant.

There was no agreement on the task force to recommend any ~~steps~~ modifications to existing ICANN policies regarding proxy services based on the information available to the Task Force.

Instead, through an appropriate mechanism, further research should be conducted on the use of "proxy registration services" within the framework of Sec. 3.7.7.3 of the RAA, including but not limited to the following issues:

- the rate of uptake of such services, their cost, and consumer response to them;
- what steps are taken to ensure the proxy service provider collects (or has immediate access to) accurate, complete and current contact information on all registrants taking advantage of such services?
  ~~*(This question does not make sense to me. The proxy provider is the registrant, and is usually making sure that their contact information is "accurate.")*~~
- the circumstances under which contact information of the actual registrant is disclosed pursuant to the RAA provision (i.e., the "evidence of actionable harm" scenario) and the consequences of such disclosures;
- how registrants are notified when the withheld data is released to third parties;
- the impact of such services on registrar portability;
- scalability of such services;
- concerns raised by customers regarding disclosure of data;

- complaints about registrar proxy or 3rd party proxy services, including complaints to or by law enforcement officials;
- contractual terms between registrants and proxy services.
- Effect of proxy situations on the stability of domain name registrations – what happens when a proxy goes out of business, and the "actual" registrant is unknown to the registrar?
    - Usefulness of proxy services to enable anonymous free speech.

The results of such research could be used to:

- develop a set of best practices for the operation of such services; and/or
- initiate a policy development or other appropriate process toward changing the terms of Sec. 3.7.7.3, if warranted.

Further work should also be conducted on the feasibility of requiring registrars to provide e-mail forwarding services to registrants, and the impact of such a requirement upon registrant privacy and contactability. As a first step, the research agenda outlined above could be expanded to study the operation of such services to the extent they exist today.

3.3 Local Law

ICANN should develop and implement a procedure for dealing with the situation where a registrar (or registry, in thick registry settings) can credibly demonstrate that it is legally prevented by local mandatory privacy law or regulations from fully complying with applicable provisions of its ICANN contract regarding the collection, display and distribution of personal data via Whois. The goal of the procedure should be to resolve the conflict in the manner most conducive to stability and uniformity of the Whois system. In all cases this procedure should include:

- Written notification by the affected registrar/registry to ICANN with a detailed report which includes but is not limited to:
    - The law or regulation that causes the conflict.
    - The part of the Whois obligation in question.
    - The steps that will have to be taken to cure the conflict.
- If data elements are removed this must be notified to the requester by the insertion of standardized notice in the Whois results advising the requester of the problem and, if possible, directing requester to another source or alternative procedure for obtaining access to this data element.
- Prompt notification from ICANN to the public informing it of the change and of the reasons for ICANN's forbearance from enforcement of full compliance with the contractual provision in question. .

- The changes must be archived on a public website for future research

~~In addition, the procedure should ordinarily be initiated by the following steps~~, E~~e~~xcept in those cases arising from a formal complaint by a local law enforcement authority that will not permit consultation with ICANN prior to resolution of the complaint under local law, the procedure should be initiated using the following steps:

- prompt notification by the affected registrar/registry to ICANN with detailed summary of the problem arising including:
  - The law or regulation that causes the conflict.
  - The part of the Whois obligation in question.
- consultation by the registrar/registry with ICANN and other parties (which may include government agencies) to try to resolve the problem/ remove the impediment to full compliance with contract.

3.5 Publication of Data

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

a) Technical and operational details about the domain name should continue to be displayed to the public on anonymous basis. Providing the name and country for both the registrant and administrative contact may also be appropriate in the interest of balancing contractibility and privacy concerns for publicly available information. Further contact details for the registrant and administrative contact would only be available in one or more protected tiers.
b) Registrants should have the option to direct that some or all of their protected data be displayed to the public.[1]
c) Those meeting the requirements to access protected information should be able to obtain it in a timely manner.
d) Those seeking access to protected information should identify themselves in a verifiable manner. Once identified, the user would be issued a portable credential, rather than needing to verify their identity on a registrar-by-registrar (or even registry-by-registry) basis.
e) The system should be affordable, both for implementers and users.

[1] Registrants who do business with the public, for example, may wish to publish their contact information so that consumers have confidence in who they are dealing with. Also, digital certificate providers typically use Whois data to issue digital certificates, so they may require registrants to publish a complete set of data as a condition for issuing a certificate.

f) There must be a legitimate use for each instance of access of protected data.
g) Registrars and registries should continue to have full access to the WHOIS data for technical and operational purposes.

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

a) What process of notification to registrants should take place when their protected data is accessed other than in circumstances required by law or contract?
b) What contact data should be shown in the protected tier?
c) What are the mechanisms available for identifying and authorizing those requesting access to protected information? Are those mechanisms fast? Are they affordable? Are they online?

4. OTHER ISSUES

CRISP - MC

5. IMPACT OF RECOMMENDATIONS

[Probably not added until final report.]

6. OUTREACH EFFORTS

6.1 Public comments on terms and conditions

After the initial publication of the task force's terms of reference, public comments on the terms of reference were solicited. Five responses were received. Four of the responses were essentially identical in content. These responses were posted by John Lawford of the Public Interest Advocacy Centre, Barbara Simons, the Past-President of the Association of Computing Machinery, Philippa Lawson of the Canadian Internet Policy and Public Interest Clinic, and Andriy Pazyuk of Privacy Ukraine. The text of these comments read as follows:

> No where in this Task Forces' description of work is there any reference to the existence of laws that protect privacy and freedom of expression in the world. We submit that this Task Force will be unable to properly perform its review of the processing of the data elements of the WHOIS database without an evaluation and clear understanding of the requirements of these laws.
>
> Proposed changes to Task Force 2 Description of Work:
>
> 1. After "The purpose of this task force is to determine" (p. 2) we strongly recommend adding a new first point:
>
> "a) Whether asking domain name owners to provide personal information is consistent with laws protecting privacy around the world?"

a) then becomes b), b) becomes c) and c) becomes d).

2. To the "Tasks/Milestones" section, we strongly recommend adding a new first Task:

"1) Document existing privacy and freedom of expression laws and regulations that are applicable to the domain name system and WHOIS data. Existing summaries of such laws, as well as materials already published by government groups, should provide an accessible base of information. Evaluate whether changes in the WHOIS data collection should be made to bring ICANN's data notification, collection, disclosure and treatment methods into conformance with existing legal frameworks."

Number 1 becomes 2, 2 becomes 3, 3 becomes 4, 4 becomes 5 and 5 becomes 6.

3. Edit existing Task #2 as follows:

" 2. Conduct an analysis of the existing uses of the registrant data elements currently captured as part of the domain name registration process. Develop a list of data elements about registrants and their domains that must be collected at the time of registration, taking into account applicable privacy and freedom of expression laws, as well as security and stability considerations."

The fifth comment was received from Mike Lampson of The Registry at Info Avenue. His comment was:

I do not believe that there should be any individual identity information shown in the public Whois, port 43 or otherwise. This would include e-mail addresses and phone numbers. For access to this information a "back door" could be mandated to allow law-enforcement, inter-Registrar transfers, or other legitimate users to acquire this information in a non-bulk fashion.

If this were to occur, ICANN or another non-government organization would need to manage the access rights to this "back door". It makes no sense for a representative of a law-enforcement agency (for example) to contact 130 different Registrars to gain access to Whois information.

As for what appears to the public in Whois, I would like to see only the technical information such as Creation Date, Expiration Date, Nameservers, etc. along with the Name and Geographic location (City, Province and Country) of the Registrant. If the Registrant Name is an individual person's name and not a business, government or non-profit, the name should be obscured with some message such as "Registered for personal use".

6.2 Data gathering process

Initially convened on 8 December, 2003, Task Force 2 engaged its work in a serious and diligent manner. The Task Force held weekly meetings and established a schedule for addressing the milestones outlined in the Description of Work.

Task Force 2 developed several resources from existing data: A chart of Whois data elements required and displayed according to registry agreements; A review of the online notification practices of the top 20 registrars (in terms of number of registrants) for whois data uses and requirements; A review of the Montreal Whois workshops for relevant discussions regarding Whois data elements collection and display.

Additionally, the Task Force prepared several surveys, each aimed at a specific audience, to collect information from the GAC members, ccNSO members, Registrars, and from

the GNSO constituencies. Responses to these surveys were extremely limited.

The Task Force also utilized resources produced outside of ICANN, including the 2003 OECD report: Privacy Online.

Constituency statements were received from all GNSO constituencies, and from the At-Large Advisory Committee. Using the statements and other materials, the Task Force members worked cooperatively through discussion and debate to prepare the Preliminary Report.

7. TASK FORCE VOTE

[To be inserted.]