

# 1. INTRODUCTION

The WHOIS service dates back at least to 1985 and, as defined in RFC 954, provides a “directory service to Internet users”. Today the WHOIS “directory” includes contact information for tens of millions of domain names, and is used for a wide variety of purposes by network operators, business of all kinds, law enforcement, consumer protection agencies, and members of the public. Through its contracts, ICANN requires registries and registrars to gather and display both technical information and contact details for all registrants. As an increasingly diverse range of both registrants and WHOIS data users have begun making use of the domain name system in recent years, situations have arisen where a registrant’s contact information may be considered sensitive, and calls have been made for better privacy protections within the WHOIS system. This Task Force was chartered to examine the manner in which data is both collected and displayed. We make a number of recommendations that allow the WHOIS service to continue to serve its valuable contactability function, while providing protection for the privacy needs of domain name registrants where appropriate.

## 1.1 Previous Discussion

WHOIS has been a topic of interest and focus for ICANN since its early days. Following up on the work of a WHOIS Committee convened by ICANN staff to give advice on implementation of WHOIS for the .com/.net/.org domains as required under the RAA, the DNSO (Domain Name Supporting Organization, the precursor to the GNSO) created a Names Council committee. Based on the recommendations of that committee, the DNSO created a task force, with the terms of reference: “Consult with the community with regard to establish whether a review of questions related to ICANN’s WHOIS policy is due and to recommend a mechanism for such a review”. This initial task force was originally composed of representatives from all constituencies, including the ccTLDs and the General Assembly, and was later expanded to include up to three representatives of each of the constituencies of the DNSO and of the General Assembly. The task force launched a survey of WHOIS and its use, analyzed 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 finding and analysis, and initial Task Force’s membership can be found at

<http://www.dnsso.org/dnsso/notes/20021015.NCWhoisTF-interim-report.html>

and the Task Force's membership at

<http://www.dnsso.org/clubpublic/nc-whois/Arc00/msg00000.html>

In order to meet its mandate of consulting broadly with the community, in addition to the survey and analysis of the responses, the initial task force undertook extensive outreach to various experts and groups, in order to inform and provide 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 was prepared on November 30, 2002<sup>1</sup>. Public comments were solicited until December 8, 2002<sup>2</sup>, and a (revised) final Policy Report published in December, 2002, proposing both consensus policy and enhancements in ICANN's enforcement of existing obligations in two areas: Accuracy<sup>3</sup> and Bulk access<sup>4</sup>.

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 task force report and reopened the report for further comment by constituencies and the community. Also at the Amsterdam meeting, the Council also established an Implementation Committee with a deadline of January 31, 2003.

The initial WHOIS task force recommended a number of consensus policies that were, after revision by the Implementation Committee<sup>5</sup> and review by the task force<sup>6</sup>, adopted by the GNSO Council and the ICANN board:

1. WHOIS Data Accuracy
  1. WHOIS Data Reminder Policy
  2. Interaction between deletions of domain names due to inaccurate WHOIS data and the the Redemption Grace Period.
2. Bulk Access
  1. Use of Bulk Access WHOIS data for marketing purposes should not be permitted, regardless of the medium used for marketing.
  2. Users who license bulk access to WHOIS data must agree not to sell or redistribute the data except as included in "value-added products" that do not permit extraction of a significant portion of the data. (I.e., the clause specified in RAA 3.3.6.5 is now mandatory.)

The recommendations of the initial task force<sup>7</sup> included the continuance of work by Council in several areas. These were not presented as consensus policy but as recommendations to Council for consideration in the further work of Council related to WHOIS.

The final consensus policy recommendations, and other findings of the initial task force, can be found in the Final Report of the GNSO Councils WHOIS TF on Accuracy and

---

<sup>1</sup> <http://www.dnsso.org/dnsso/notes/20021130.NCWhoisTF-accuracy-and-bulkaccess.html>

<sup>2</sup> <http://www.dnsso.org/dnsso/dnsocomments/comments-whois/Arc02/>

<sup>3</sup> <http://www.dnsso.org/dnsso/notes/20030110.GCWhoisTF-accuracy.html>

<sup>4</sup> <http://www.dnsso.org/dnsso/notes/20030110.GCWhoisTF-bulkaccess.html>

<sup>5</sup> [http://www.dnsso.org/dnsso/notes/20030130.WHOISImpFinalReport\\_v4.html](http://www.dnsso.org/dnsso/notes/20030130.WHOISImpFinalReport_v4.html)

<sup>6</sup> <http://www.dnsso.org/dnsso/notes/20030219.WhoisTF-accuracy-and-bulkaccess.html>

<sup>7</sup> <http://www.dnsso.org/dnsso/notes/20030219.WhoisTF-accuracy-and-bulkaccess.html>

Bulk Access, Feb. 6, 2003 approved by the Council<sup>8</sup>, and forwarded to the ICANN Board on 20 February 2003.

The Implementation Committee report can be found at <http://www.dns0.org/clubpublic/nc-impwhois/Arc00/msg00057.html>. The Council received the Implementation Committee report and included its recommendations in the final Report forwarded to the Board 20 February 2003.

## 1.2 Genesis of the Task Force

Following the work and recommendation of the initial WHOIS task force, the Council discussed how to proceed on WHOIS issues. The Council did not consider the further recommendations of the initial task force definitive, and thus, there may appear to be something of a discontinuity between the recommendations for further work provided by the initial WHOIS task force and the ongoing GNSO task force work on WHOIS. Some areas suggested by the previous task force 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. At its meeting in Rio de Janeiro<sup>9</sup>, Council decided to ask ICANN staff to prepare a staff manager's report on WHOIS privacy that would consolidate reports received from the WHOIS Task Force<sup>10</sup> and NCUC<sup>11</sup>. The Council also agreed to schedule discussion of remaining accuracy issues for six months after the implementation of the WHOIS recommendations before the board in Rio de Janeiro, or until completion of the policy development process on privacy, whichever comes first. As suggested in the Staff Manager's Issues Report on Privacy Issues Related to WHOIS<sup>12</sup>, the Council decided to create a WHOIS Privacy Steering Group, in order to examine what issues should be addressed by further WHOIS task forces of Council. Council also requested the ICANN President to organize a workshop for the Montreal meetings which should incorporate the GNSO constituencies as well as the Government Advisory Committee and other groups.<sup>13</sup> The WHOIS Steering Group attempted to identify a neutral chair, but given time constraints, the group agreed to conduct their work with Bruce Tonkin, the chair of Council, as the Chair of the group. The group included members from all constituencies, liaisons from ALAC, ccTLDs, GAC and Council members appointed by

---

<sup>8</sup> <http://www.dns0.org/dns0/notes/20030220.GNSOteleconf-minutes.html>

<sup>9</sup> <http://www.dns0.org/clubpublic/council/Arc12/msg00247.html>

<sup>10</sup> <http://www.dns0.org/dns0/notes/20030311.WhoisTF-privacy-issues.pdf>

<sup>11</sup> <http://www.dns0.org/dns0/notes/20030310.Whois-PrivacyIssuesReport.pdf>

<sup>12</sup> <http://www.icann.org/gns0/issue-reports/whois-privacy-report-13may03.htm#RecommendedProcessforProceeding>

<sup>13</sup> See minutes of GNSO Council meeting on 22 May 2003 –

<http://www.dns0.org/dns0/notes/20030522.GNSOteleconf-minutes.html>

the Nominating Committee<sup>14</sup>.

The group worked to identify priorities for the community based on a review of the constituencies and the stakeholders perspectives.<sup>15</sup> This work provided the basis for Council's chartering of further Task Force work on WHOIS.

The Privacy Steering Group held several conference call meetings, and met face to face at ICANN meetings. Parallel to the steering group's work, ICANN hosted two workshops in 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 included the OECD, the U.S. Federal Trade Commission, the US Department of Justice, the European Commission, WIPO, data privacy experts from Europe, industry experts in intellectual property issues affected by WHOIS, and ccTLD managers who were invited as experts on how particular issues are dealt with within their ccTLD<sup>16</sup>.

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 the formal decision of the At-Large Advisory Committee to raise the review of data elements collected and displayed as an issue for policy development, 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 task forces on WHOIS, with the assumption that the alignment of recommendations will take place in Council. WHOIS Task Forces 1 and 2 were launched on 22 October 2003 and Whois Task Force 3 on 23 October 2003; the Descriptions of Work (DOW) of each Task Force is available at:

WHOIS Task Force 1	<a href="http://gnso.icann.org/issues/whois-privacy/tor.shtml">http://gnso.icann.org/issues/whois-privacy/tor.shtml</a>
WHOIS Task Force 2	<a href="http://gnso.icann.org/issues/whois-privacy/tor2.shtml">http://gnso.icann.org/issues/whois-privacy/tor2.shtml</a>
WHOIS Task Force 3	<a href="http://gnso.icann.org/issues/whois-privacy/tor3.shtml">http://gnso.icann.org/issues/whois-privacy/tor3.shtml</a>

### 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

---

<sup>14</sup> A list of members is available at <http://gnso.icann.org/issues/whois-privacy/membership-liaison-update-19sep03.shtml>

<sup>15</sup> <http://gnso.icann.org/issues/whois-privacy/table-whois-privacy-issue.shtml>

<sup>16</sup> See

<http://gnso.icann.org/issues/whois-privacy/whois-workshop-03feb04.shtml>  
for presentations and agenda for workshops at Montreal and Tunisia

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.

The Task Force recommends a number of changes to current WHOIS policy that are intended to reflect this balance in a reasonable and consistent manner.. These recommendations are described in detail in section 3 of this report, but are summarized below:

- 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.
- Further inquiry should be made into proxy registration services provided by registrars and others in order to provide increased privacy for registrants.
- Registries and 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 make appropriate changes needed for it to conform to the respective local laws.
- The task force believes that a system that provides different data sets for different uses (also known as "tiered access") should be explored to see if it 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, and to determine its viability, balance of interests and financial feasibility.

## **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 A 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 description of work for Task Force 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 Task Force's 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. However, situations have arisen in which privacy laws or regulations have conflicted with WHOIS-related contractual obligations with ICANN. For example, the recently revised .name WHOIS policy which had to be changed to comply with a request of the UK Data Commissioner. In the Task 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 in case of successful complaints to the Information Commissioner.”* ([http://www.gnso.icann.org/mailing\\_lists/archives/dow2tf/msg00152.html](http://www.gnso.icann.org/mailing_lists/archives/dow2tf/msg00152.html))

The Task Force believes that there is an ongoing risk of conflict between a registrar's or registries' legal obligations under local privacy laws and their contractual obligations to ICANN.

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 conflict with a law or 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

In the Description of Work, the GNSO Council asked the Task Force: "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 protection." 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 Noncommercial Users' Constituency (NCUC) commented that Registrars should follow well-established data protection principles before collecting extensive personal data, including name, address, phone and email for registrants and administrative contacts. NCUC felt the current data elements raise deep concerns for privacy and anonymous expression, and that Registrars should be allowed to collect this data as-needed for business purposes, but not on a mandatory basis for global publication in the WHOIS directory.<sup>17</sup> ALAC's comments similarly called for limits to the collection of personal data: "What information is actually required for placing a domain name registration should be a matter of registrars' business models, and of applicable law, not of ICANN policy."

ICANN also heard calls to limit the collection of personal data at the Rome meeting and in comments, including a reference to the European Data Protection Commissioners' Article 29 Working Party, which wrote: "it is essential to limit the amount of personal data to be collected and processed. This should be kept particularly in mind when discussing the wishes of some parties to increase the uniformity of diverse WHOIS directories." ("Opinion 2/2003 on the application of the data protection principles to the Whois directories," [http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2003/wpdocs03\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2003/wpdocs03_en.htm))

The ISP, Intellectual Property and Business constituencies stated that all data elements should continue to be collected. The Business Constituency's statement noted "the continued need for all the data elements that are collected in Whois today." The ISP constituency proposed that "all [data] elements continue to be collected and displayed, for those authorized to obtain access." The IP constituency opposed elimination of any data element and suggested five others whose inclusion "would improve the usefulness of Whois data." The Registry constituency, however, did "not see a need for additional fields beyond those presently available." The registrar constituency did not comment specifically on collection of data, but did propose three lists of data elements that should be displayed to different types of requesters, including at least one elements not now

---

<sup>17</sup> The American Civil Liberties Union commented separately that the mandatory collection practices endanger protected rights of anonymous political and personal expression passionately protected under US law.  
<http://gns0.icann.org/mailling-lists/archives/tf2-survey/msg00018.html>

required to be collected or displayed under the RAA (e-mail address of registrant).<sup>18</sup>

Accordingly, the Task Force proposes the following conclusions on the issues identified in Task/Milestone 2 of the Task Force 2 Description of Work:

- There was no consensus that the data elements currently being collected should be changed. 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 whether such needs are consistent with the purpose of the WHOIS database and the reasons for collection of sensitive/personal data by registrars.
- 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 Task Force 3 rather than Task Force 2.
- 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 the Task Force. While public access to the WHOIS databases by Internet users have been a feature of the domain name system since its inception, the network was originally small and the WHOIS database was limited to the information of research and technical institutions. This data—including registrant name, address, phone and email—is now accessible to a much broader spectrum of members of the public (including on anonymous basis). With this evolution have come increasing expressions of concern about the impact of the data on personal privacy and freedom of expression infringement (outlined below).

One topic the Task Force 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 day the knotty question of the ultimate purposes of this database, and whether and how they can change.

### Findings:

- a) 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.

---

<sup>18</sup> See <http://www.gnso.icann.org/mailing-lists/archives/dow2tf/msg00202.html> (including attachment) and <http://www.gnso.icann.org/mailing-lists/archives/dow2tf/msg00217.html> for constituency statements.

- b) WHOIS data often includes personally identifiable and otherwise in the registrant, administrative contact and technical contact fields. It is the type of information that, in some other contexts, individuals, human rights organizations and businesses (such as abortion clinics) have some ability to limit and control access to (e.g. an unlisted or ex-directory phone number).
- c) Submissions to the Task Force show that WHOIS data is used for a wide range of uses. The data is widely used by network operators, businesses of all kinds, law enforcement, consumer protection agencies and members of the public for learning who has registered a domain name.
- d) Abuses of public access to Whois data have occurred and have impacted on registrant privacy. Instances of 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 have been presented to the Task Force, although the extent of such abuses has not been documented.
- e) In order to maintain the balance of contactability and privacy, which the Task Force was charged to find, a tiered access system deserves careful consideration and received extensive discussion in the Task Force. Other options that also merit consideration but received less discussion in task force deliberations to date include proxy registration services (see questions raised in section 2.2) and the ability of domain name registrants to “opt-out” of publication of WHOIS data on a case-by-case basis (as is currently the case in some ccTLDs).
- f) Some data requesters want timely, even immediate, responsiveness to their requests for WHOIS data. Some 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:

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. On the other hand, the ISPCP raised the concern that notification of the domain name holder when his/her personal data was revealed would be in conflict with ISPs’ legally mandated responsibilities in assisting law enforcement personnel would compromise ISP security and network protection efforts and would otherwise not be a viable aspect of any possible tiered system. The attention of the Task Force was also called to the example of GNR,

registry operator for .name, which adopted (with ICANN approval), but has not yet implemented, a tiered access system for Whois in .name.<sup>19</sup>

A tiered access proposal submitted to the Task Force during its deliberations called for a combination of some 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). Finally, registrars would be provided with access to the full data for technical co-ordination purposes, such as fulfilling inter-registrar transfer requests.

Other constituencies urged further explorations of other mechanisms to adjust the privacy/contactability balance, including (a) whether a system for withholding some contact data on individual registrants on a case-by-case basis due to special circumstances, already in place in some ccTLDs, could be viably extended to the gTLD environment as well as (b) the role of CRISP and other merging and relevant technical standards.

### **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

---

<sup>19</sup> The proposed .name approach to WHOIS is memorialized in Appendix O to their Registry Agreement with ICANN at <http://www.icann.org/tlds/agreements/name/registry-agmt-appo-8aug03.htm>

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 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?
- 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 3<sup>rd</sup> 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 a manner 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

Except in those cases arising from a formal complaint or contact 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.

### **3.4 Collection of Data**

The Task Forces makes no recommendation with regards to the collection of data at this time.

### **3.5 Publication of Data**

The task force believes that a system that provides different data sets for different uses

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

- a) Technical and operational details about the domain name should continue to be displayed to the public on anonymous basis. Providing some basic contact information (possibly limited to the name and country for both the registrant and administrative contact) may also be appropriate in the interest of balancing contactability 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.<sup>20</sup>
- c) Those meeting the requirements and identifying a legitimate use to access protected information should be able to obtain it in a timely manner.
- d) Those seeking access to protected information should identify themselves in a verifiable manner. Once identified, the user would be issued a portable credential, rather than needing to verify their identity on a registrar-by-registrar (or even registry-by-registry) basis.<sup>21</sup>
- e) The system should be affordable, both for implementers and users.
- f) Registrars and registries should continue to have full access to the WHOIS data for technical and operational purposes.

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

- a) What process of notification to registrants, if any, should take place when their protected data is accessed other than in circumstances required by law or contract (e.g. the provision of contact to UDRP providers during a UDRP dispute, or to another registrar during a transfer)?
- b) What contact data should be shown in the protected tier? How will the data compare with what is now available? How will the accuracy compare with what is now available?
- c) What are the mechanisms available for identifying and authorizing those

---

<sup>20</sup> 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.

<sup>21</sup> It is also desirable for these credentials be honored by all registries and registrars. However, the Task Force does not intend for this to imply that a single, centralized credentialing authority should be used. Rather, credentials would meet a commonly agreed upon set of criteria, and be issued according to well defined standards; in turn, these credentials would be honored by all registries and registrars.

- requesting access to protected information? Are those mechanisms fast? Are they affordable? Are they online? Who will administer them, using what criteria?
- d) How will the costs of implementing a tiered access system be borne?
  - e) Will existing technology standards (such as CRISP) would support such a system? If so, how?

## 4. IMPACT OF RECOMMENDATIONS

The task force intends to assess the impact of its recommendations prior to the issuance of its final report.

## 5. 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. These comments suggested that the task force's charter should be updated to consider laws that protect privacy and freedom of expression.

The fifth comment was received from Mike Lampson of The Registry at Info Avenue. His comment indicated that an individual's contact information should not be made available to the public, but only in limited circumstances through a "back door" with access rights managed by ICANN or some other non-government organization.

The full text of the public comments is available at <http://gnso.icann.org/mailing-lists/archives/dow2/>.

### 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](#). A mailing list was established, with [public archives](#), and materials prepared from work completed was posted to the GNSO website on [Whois Privacy issues](#).

The Task Force presented work-to-date in a [public workshop at the Rome ICANN meeting](#) in March 2004.

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 whose 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 and ccTLD managers](#), [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.

## 6. TASK FORCE VOTE

This report was approved for publication and public comment by a unanimous vote of the task force. However, several constituencies made comments in conjunction with their vote. Those comments are recorded as footnotes to the record of votes below.

The following representatives voted to publish this report:

- [Business Constituency](#)<sup>22</sup>

---

<sup>22</sup> The Business Constituency representative provided the following comment in conjunction with the constituency's vote: The BC records the following reservation comments to be noted in the TF records.

There are various places within the report where the BC is not in agreement with the characterization of the positions taken by the TF and reserves the right to correct these views in the final report of the TF. We will not hold up the report for these clarifications.

In particular, the BC is concerned that consideration of a "tiered approach" has been put forward without adequate assessment of "unfunded mandates" to the registrar community, nor the implications to registrants, users, or registrars. This topic does deserve immediate assessment, but we cannot support a recommendation that is not substantiated by a feasibility assessment. Our views on this have been stated in several meetings and we hope are finally captured accurately. We support studying and assessing the feasibility, impact on users, registrants, and registrars, and the costs to make such a change. Then we can determine our support for implementing this "concept".

The BC notes that there are in some cases incomplete descriptions of input from different entities of the TF, however, we believe these are omissions due to limits of time or adequate staff support, and therefore, we are not inclined to object to the move of the report for public comment, as long as it is quite clear that this is an Interim Report and should not be considered conclusive of final views of any TF participant.

The BC thanks all other members of the TF and in particular the chair for their good will, professional behavior, and personal integrity and commitment to the bottom up, consensus based policy development process that ensures ICANN's success. While we may not always agree, we do have a professional obligation and responsibility to support ICANN's policy process, and we appreciate the opportunity to work with others from the community in this process. Finally, the BC thanks the gnsso secretariat for their organizational support to the TF.

Finally, it is important to remember that we are working toward consensus based policy, that is implementable. We recognize that we have more work to do, as a TF, once we receive public comment. For instance, we have more work to do, including undertaking GAC input and advise, and Council will undoubtedly establish an Implementation working group process before we finalize our final recommendation to Council. So, we note to our fellow TF members, our commitment

- Intellectual Property Constituency
- Internet Service Providers and Content Providers
- Noncommercial Users Constituency<sup>23</sup>
- Registrar Constituency<sup>24</sup>
- Registry Constituency

Additionally, the representative of the At-Large Advisory Committee and Amadeu Abril-i-Abril, a Nominating Committee appointee to the GNSO Council who participated in the task force, voted in favor of publishing the report.

There were no votes against publication or abstentions.

Comments for the Whois Task Force 2 Preliminary Report can be submitted to: [whois-tf2-report-comments@gnso.icann.org](mailto:whois-tf2-report-comments@gnso.icann.org).

The comment archives are available at <http://gnso.icann.org/mailling-lists/archives/whois-tf2-report-comments>.

---

to work toward consensus policy recommendations.

Thanks to our chair for his leadership and significant amount of work, and thanks to several TF members who did really terrific amounts of work and consultations to get us as a TF to this point.

<sup>23</sup> The Noncommercial Users Constituency representative provided the following comment in conjunction with the constituency's vote:

The Noncommercial Users' Constituency approves the preliminary TF2 report and supports its publication in full to the public for comment. We note the following concerns and reservations regarding Section 3.5 and throughout the report, to be recorded with our vote:

The Noncommercial Users' Constituency approves of the concept of a Tiered Access With Balance, in which the rights of the data subjects (domain name holders) are clearly balanced with the rights of the data recipients (e.g., intellectual property owners). In doing so, we submit that there must be a clear distinction of sensitive and non-sensitive data, that domain name holders must receive immediate notification when data is released (in most cases), and that the system must avoid any White List (unlimited access to certain parties merely because they are known users).

<sup>24</sup> The Registrar Constituency representative provided the following comment in conjunction with the constituency's vote:

- 1.) what exactly must the registrant consent too?
- 2.) what happens if the registrant does not consent to the display of certain parts of his data?
- 3.) what happens if the registrant does not consent to certain methods of display of his data?
- 4.) what happens if the registrant does not consent at all?
- 5.) what happens if the registrant withdraws his consent.