Define the purpose of the Registered Name Holder, technical, and administrative contacts, in the context of the purpose of WHOIS, and the purpose for which the data was collected.

Use the relevant definitions from [Exhibit C of the Transfers Task force report](http://www.icann.org/gnso/transfers-tf/report-exhc-12feb03.htm)as a starting point:   
(from <http://www.icann.org/gnso/transfers-tf/report-exhc-12feb03.htm> ):

Typically, third parties with specific inquiries or concerns will use contact records to determine who should act upon specific issues related to a domain name record. There are typically three of these contact types associated with a domain name record, the Administrative contact, the Billing contact and the Technical contact. Contact, The administrative contact should be able to answer non-technical questions about the domain name's registration and the Domain Holder. In all cases, the Administrative Contact is viewed as the authoritative point of contact for the domain name, second only to the Domain Holder.

Contact, Billing: The billing contact is the individual, role or organization designated to receive the invoice for domain name registration and re-registration fees.

Contact, Technical: The technical contact is the individual, role or organization that is responsible for the technical operations of the delegated zone. This contact likely maintains the domain name server(s) for the domain. The technical contact should be able to answer technical questions about the domain name, the delegated zone and work with technically oriented people in other zones to solve technical problems that affect the domain name and/or zone.

Domain Holder: The individual or organization that registers a specific domain name. This individual or organization holds the right to use that specific domain name for a specified period of time, provided certain conditions are met and the registration fees are paid. This person or organization is the "legal entity" bound by the terms of the relevant service agreement with the Registry operator for the TLD in question."

**OPoC Proposal**

"Under this proposal, the administrative and technical contacts would no longer be displayed within the Whois system. As a result, they would no longer have a purpose within the context of Whois."

"This proposal introduces the Operational Point of Contact, which would be collected by registrars and displayed in response to Whois queries regarding specific domain names. The purpose of the operational point of contact is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name. At a minimum, this must include the resolution of issues relating to the configuration of the records associated with the domain name within a DNS name server. The operational point of contact may also be capable of resolving additional types of issues based on an agreement with the registered name holder to do so."

"The purpose of the operational contact is to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name."

**Summary of task force discussion (including proposal for access to data)**

Representatives of the registrar constituency proposed that such data could be made available by contacting the registrar of record for the domain name, without any new rules or policies, but be made subject to best practices. Today, registrars handle many requests for other information not published in the Whois, and they expect to handle requests to data removed from the Whois in a similar manner.

**Statement of the Commercial and Business Users Constituency**

Recommendation: Any proposal to modify the existing WHOIS policy related to data displayed and access to data must include a process for access to non displayed data before changes in the existing practices are introduced.

One approach that could merit study is the recognition that there are hundreds of accredited registrars, and that any approach needs to take into account the burden on legitimate users of WHOIS. It may be appropriate to examine the creation of a "white list" for legitimate stakeholders who need access to deal with "legitimate" purposes, such as network attacks; phishing; pharming attacks; trademark collisions, etc.

Recommendation: The OPOC proposal should be elaborated to include a pre validation of the completeness and accuracy of contact details of the OPOC at the time of registration. The RAA should also provide for periodic checking of the OPOC details and a standardized notice to the registrant, to remind them to verify the accuracy of their OPOC details, and of consequences of providing inaccurate, or failing to correct such data, such as suspension/loss of registered name.

Therefore BC supports the concept of establishing a process whereby an individual, or appropriate non commercial service entity can apply for an opt-out for the inclusion of their contact data in a publicly accessible WHOIS if their safety and security cannot be protected otherwise, as provided by the Special Circumstances Proposal.

Recommendation: The SCP should be elaborated to include a pre validation of all contact details at the time of registration for any party determined to be eligible for SC. The third party who holds the data should be required to provide accurate data for themselves and to attest that they have verified and maintain accurate contact data for the registrant. The RAA should also provide for periodic checking of the SC registrant data and procedures to require updates, or corrections.

The BC agrees that the proposal needs to be examined for scalability to the gTLD non sponsored space. In general, the BC supports the concepts provided in the SCP to rely upon outsourcing of the special circumstances application process to independent third-party vendor(s), possibly on a regionalized basis, ensuring adequate funding and outlining a simple and clear process for the application, designation and appeal of "special circumstances" request(s).

Analysis of how the issue would affect the constituency; including any financial impact on the constituency

The BC's interests are harmed by the lack of accurate WHOIS data and will be harmed by lack of access to WHOIS data, if public access to WHOIS data is changed, and if there is no suitable substitutes to ensure that legitimate users have timely access to accurate WHOIS contact data, so that they can deal with network attacks, trademark infringements; phishing and pharming attacks, as well as undertake normal use of the WHOIS database related to checking for availability of registerable names for use in setting up new web sites.

The OPOC proposal is anticipated to have an ongoing negative financial impact to users of WHOIS data, who rely on access to WHOIS data to quickly identify and contact the party responsible for cyber squatting, phishing, pharming, network attacks, and trademark infringements.

A move to web based access coupled with improved contractual terms for bulk access will represent the least invasive change to users, but will curtail data mining in displayed data. Thus, this change, as recommended by the Business Constituency, provides improvements to WHOIS but without the associated harms to the interests of the Business Constituency's members.

**Statement of the Intellectual Property Constituency (IPC)**

The many legitimate uses that constituency members make of Whois data are well documented in previous submissions. For most of these uses, especially those regarding protecting the intellectual property rights of companies, non-profit institutions, trade associations, and individuals, ready access to the full range of Whois data is critical. This access enables intellectual property owners to quickly contact the party responsible for the registration or use of a domain name that involves infringement of trademark or copyright, cybersquatting, or other illegal behavior. In most cases, this quick contact leads to a prompt resolution of the problem, without the need to invoke the UDRP or more formal legal processes. In those cases which do proceed to a UDRP complaint, civil litigation, or a criminal investigation, the data currently available in Whois is often essential to effective enforcement.

Basically the same holds true when constituency members access Whois for other legitimate purposes such as combating or preventing online frauds, conducting due diligence in mergers and acquisitions, and the like: quick access to contact data on registrants and their administrative and technical agents facilitates quick resolution of problems in the great majority of cases, which is in the best economic and legal interest of all parties concerned. When a quick resolution is not possible, Whois data plays an important role in the service of legal process, further investigations, and other follow-on activities.

Under the OPOC proposal, most of the data in Whois that enables these quick contacts and that supports these follow-on activities would no longer be available to IPC members (or any other member of the public). Only the registrant's name and country/state or province would be published. Instead, the intellectual property right holder would have to work through whomever the registrant had designated as his/her/its "operational point of contact." This entity's "purpose" would be "to resolve, or to reliably pass on data to resolve, operational issues relating to a domain name." But the proposal raises far more questions than it answers about how an intellectual property right holder would achieve the quick contact with the registrant which the current system of public access facilitates.

**Statement of the Registry Constituency**

RyC believes that complete anonymity, even if it were possible to achieve, is not a viable option as a mechanism for privacy protection.

Proposals for "tiered access" are examples of mechanisms for this purpose. These appear to offer significant improvements in the protection of personal privacy, as compared to the situation today. RyC recommends that the task force direct its future efforts to finding a workable form of tiered access that might be acceptable to most, if not all, interested parties. (RyC's comments on a proposal for another mechanism, the "Special Circumstances Proposal" are set forth below.)

THE ISSUES NOT AGREED

The two issues not agreed, *i.e.,* the purpose of WHOIS contacts, and the question whether there should be a change in data from that now published, are unlikely ever to be the subject even of rough consensus among the interested parties.

The GNSO resolution on the subject of the purpose, adopted on April 12, 2006, reads as follows:

*"The purpose of the gTLD WHOIS service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server."*[[11]](http://gnso.icann.org/en/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm" \l "_ftn11" \o ")

This resolution is supported by RyC with the qualification that it does not preclude access to data by law enforcement and other parties having legitimate needs for access.

RyC believes that a decent respect for registrants' interests in protection of personal privacy demands a change in the type of data published in the WHOIS service. There is, of course, a difference between the types of data collected by registrars, and the types of data published in the WHOIS service. RyC generally supports the concepts underlying the Registrar Constituency's OPoC proposal (although there are some practical concerns addressed below). Registrars have their own business needs for collection of registrant data, and should be able to make decisions primarily based on these needs and on the legal requirements of the jurisdictions where they operate.

RyC strongly believes that there is no acceptable reason for publication of an individual's personal data such as home address, phone number or email address, whether by a registry or registrar. To the extent that such data is needed for law enforcement purposes or for the resolution of conflicts such as intellectual property, the appropriate means to meet these needs should be a tiered access process.

Adoption of the positions advocated by RyC would assist the members of the RyC in fulfilling their legal obligations in their respective jurisdictions, and would be of significant benefit through lifting burdensome contractual requirements. The impact of WHOIS changes is larger for thick registries than it is for thin, and the impact on sponsored registries can be more significant than on unsponsored registries. Any major changes would likely have considerable impact on registries and especially on registrars, in time, money and resources.

**Statement of the Non Commercial Users Constituency**

The Noncommercial Users Constituency (NCUC) believes that ICANN policies governing the publication of Whois

data must be reformed, and quickly. The Operational Point of Contact Proposal ("OPoC Proposal") presented in this

Whois Task Force Report is not perfect, but it is the only way to bring some consensus and closure to a problem that

has festered for too long.

NCUC believes that the Operational Point of Contact (OPoC) Proposal is a judicious compromise that feasibly balances constituency input with the original purpose of Whois, ICANN's Mission and Core Values, and the GNSO Council's April 12 decision.

On the question of access to data not published, NCUC agrees with the registrars that there are existing procedures

for requesting such data from the registrar of record. But we would like to see the rights of individual registrants made

clearer and stronger, and we do not believe that registrars should be able to handle any form of disclosure at their

own discretion. We believe that disclosure pursuant to law protects the registrars, registries and ICANN.  Registrar

policies should follow those that already exist in their countries for disclosure of unlisted telephone numbers, email

and chatroom identities, etc.

At this time, NCUC cannot support a proposal to allow unpublished Whois data to be accessed by anyone who signs

a contract agreeing to limitations on the use of the data. Although we recognize that sufficiently restrictive terms and

conditions might make such a "tiered access" contract worth considering, we believe that such a policy of access

must *follow* implementation of the OPoC proposal and be part of a *new* and *separate* PDP. Discussion of such a

proposal must be linked to discussions about what data is collected by registrars; what fees should be charged to

users of a tiered access regime (fees being justified both to finance the system, assign costs to cost-causers, and to

discourage misuse of tiered access for unmotivated "fishing expeditions"); what limitations should be imposed on use

and transfer of the data; what mechanisms would be used to enforce the contract; what kind of entities would be

eligible for such contracts, what type of penalties should be imposed for abuse, and what types of access are allowed

under national laws.

NCUC has always maintained that better privacy protection can pave the way for more accurate data, and therefore supports the OPoC proposal's accuracy improvement measures. Our support for improved accuracy is still contingent, however, upon a movement away from indiscriminate publication of sensitive contact data.

**Statement of the Internet Service Providers and Connectivity Providers Constituency**

The ISPCP stresses the need for balance in adoption of changes, respect for earnest privacy concerns and concern over the limiting access as a means to conceal the identity of organizations or persons involved in illegal or criminal activity.

Internet Service Providers (ISPs) use Whois data for a variety of needs, but most readily to prevent and detect sources of security attacks on their respective networks and servers; to identify sources of consumer fraud, spam, phishing and denial of service attacks; and to support technical operations of their connectivity services. Moreover, since ISPs are a primary source for information on the investigation cyber-crimes, Whois data allows ISPs or law enforcement agencies to obtain some information on the subjects of the investigation that is outside the reach of ISPs but integral to obtaining the resolution of law enforcement needs.

**Full Task Force Terms of Reference**

ICANN has agreements with gTLD registrars and gTLD registries that require the provision of a WHOIS service via three mechanisms: port-43, web based access, and bulk access. The agreements also require a Registered Name Holder to provide to a 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; the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and the name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name. The contact information must be adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.

A registrar is required in the Registrar Accreditation Agreement (RAA) to take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

The goal of the WHOIS task force is to improve the effectiveness of the WHOIS service in maintaining the stability and security of the Internet's unique identifier systems, whilst taking into account where appropriate the need to ensure privacy protection for the Personal Data of natural persons that may be Registered Name Holders, the authorised representative for contact purposes of a Register Name Holder, or the administrative or technical contact for a domain name.

**Proposal to the Task Force by Avri Doria, Milton Mueller, Robin Gross and Wendy Seltzer**

**I) The purpose of Whois**

It is widely accepted that the original gTLD Whois service was used for the purpose of coordinating technical actors as they sought to resolve operational issues related to the security and stability of the DNS and a well-functioning internet.

The importance of this original, technical purpose was reaffirmed in the GNSO council's recommended[[12]](http://gnso.icann.org/en/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm" \l "_ftn12" \o ") definition on the purpose of Whois:

*"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server."*

The scope of use of published Whois data has increased considerably beyond this over time, a subject that has already been substantially considered by the GNSO Whois Task Force and Council. The scope of use of the internet has also changed over time, as have the management tools used to administer these uses.

The public debate over Whois is overlooking a very important fact. In all Whois uses related to the security and stability of the DNS, the truly useful information is not the contact information for the domain name registrant, it is the name server information for the name in question. Unfortunately, neither the contact information nor the name server information in Whois is reliable or useful, because authoritative information about DNS resources doesn't live in a gTLD database, it lives inside the DNS itself.

The validity of the data in a gTLD Whois database has no impact on the operational integrity of the DNS.

Due to this disconnect between DNS and Whois, network systems managers rarely rely on gTLD Whois service when they seek to investigate or resolve serious network operations and technical coordination issues. An entirely different set of tools and resources that relies on authoritative data have evolved that support the requirements of these types of users. For example, a network administrator might use "dig"[[13]](http://gnso.icann.org/en/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm" \l "_ftn13" \o ") or "nslookup"[[14]](http://gnso.icann.org/en/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm" \l "_ftn14" \o ") to determine the source of a DNS problem or the network location of a mail server being abused to send spam email. All of these tools are publicly available at no charge, internet standards based, and in widespread use.

Furthermore, from a network management perspective, not only is the data in the DNS resource records more authoritative (and therefore useful), it is also more comprehensive. A typical DNS record can include information about the network location of any and all web servers, email servers and other resources associated with a specific domain name ? at all sub-levels associated with the specific DNS entry (i.e., the second, third and fourth levels of the domain hostname). The gTLD whois service contains none of this important information.

When DNS data is used in conjunction with the IP Address Whois data sourced from providers like ARIN or RIPE, a network administrator is able to form a fully authoritative view of not only the services associated with a specific domain name, but also the identity of the entity that physically hosts those resources and how to contact that entity. All of this data exists outside the gTLD Whois system.

**Technical coordination in the real world**

Most technical coordination of DNS administration, abuse and network management issues occurs without ICANN's involvement. Private sector coordination is more likely through CERT, NANOG, Reg-OPS and other forums, than those operated by ICANN. These initiatives are often ad hoc and key players do often not understand the importance and value of participation. This is an area where small improvements in the overall level of cooperation between the various initiatives would lead to substantial improvement in the overall security of the internet and DNS infrastructure.

**Proposal to the Task Force by Marilyn Cade**

Attempts to define the original purpose of WHOIS services encounter many disputes, according to who is speaking, whether it is a business user; an ISP/connectivity provider; a privacy activist/organization; a registry or registrar, law enforcement agency, a sys-adm dealing with network attacks; a legal advisor inside/outside a corporation.

Much of the debate on WHOIS centers around whether and what data should be publicly displayed. There has been less disagreement about the need for accurate data, and that there are legitimate uses for contact data. There are some different views on which 'Internet tools' or other resources might substitute for access to accurate WHOIS data, but little exploration and there is no agreement on whether such 'tools' are indeed substitutes.

The proposal seeks to create significant changes to the display method, and therefore the access to public displayed data. Such changes can help to curtail, if not eliminate alleged and/or actual data mining and harvesting of email and telephone numbers. In addition, this proposal would, if implemented, create strict limits to how bulk access and Port 43 access to WHOIS data is granted, and the creation of a 'white list' of authorized uses, and users for bulk access.

All WHOIS access should be changed in all WHOIS services to web based access. Such web based services should include an Image Verification Check (IVC) of sufficient security strength so that the random letters generated are not easily machine readable. The requirement to implement such a system should become a part of consensus policy, but the mechanism that each registrar/registry uses for IVC should be of their selection, as long as sufficient security is ensured.

All bulk access should be moved to ICANN managed contractual terms for access, with an application/accreditation process for parties allowed to have such contracts. This consideration was first proposed by the initial DNSO WHOIS Task Force and deserves further consideration. The 'white list' should be maintained by ICANN, and will require a suitable cost based fee to bear the cost of implementation. Criteria for application/accreditation will need further examination, and should be posted for public comment as part of the development of said criteria. ICANN should develop standard terms and conditions for the agreements, and ICANN should provide enforcement when they are violated and complaints are received from the registry/registrar for such violation, including removing the accreditation for the 'white list'; such as charging additional fee penalties, etc.

In general, parties who need bulk access for legitimate purposes are trademark and other firms that provide trademark defense or portfolio management services. Consensus policy may be needed to establish the framework for collaboration to achieve a balanced solutions and terms. ICANN operational staff will play a significant role in helping to develop and implement a suitable approach.

This approach does need further exploration with law enforcement and consumer protection authorities to ensure how best to address their need for port 43 access or bulk access.

While estimates vary, approximately 75%+ of these are registered in gTLDs, and approximately 25% are registered in country codes. It is clear that while some users may find identity in a domain name as an individual, the vast majority of Internet users do not rely on domain names, but rely on ISPs, web hosters, and connectivity providers to provide them with identity online via web email addresses, individual web pages, etc. In short, what and who will support identity on the Internet is yet to be determined and continues to evolve.