Issues report – WHOIS privacy

Introduction

The present document is an extension to the issues report on privacy which had been provided earlier by the Task Force. In addition to enumerating a number of issues, we also present an attempt to identify various perspectives relevant for the discussion, and to identify a number of "dimensions" in which WHOIS policy can be adjusted.

Background

To be done.

Viewpoints on WHOIS privacy

The Contribution of globally, publicly accessible WHOIS information to identy theft and other fraud

The U.S. Federal Trade Commission (FTC) plays a critical role both in the investigation of consumer fraud and in the protection of consumers from fraud. According to the FTC's website, "The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them." [See, for example, http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm]

In this vein, the FTC advises consumers not to disclose personal information, and if consumers choose to disclose personal information, they should know who is collecting the information, why the information is being collected, and how it is going to be used. Not only does the global, public accessibility of WHOIS data contradict FTC's advice, but the consumer, as a domain name registrant, is stripped of these abilities, as the registrant has no way of knowing who collected his/her WHOIS data, why the information was collected, and how the collector intends to use the information. Further yet, with the enforcement of the accuracy of WHOIS data, as is recommended by the WHOIS Task Force, consumers will not even have a choice on whether to disclose their personal information. The alternative to relinquish a domain name is not giving consumers a genuine choice, and instead infringes on Internet free speech.

The global, public accessibility of WHOIS data imposes risks on domain name registrants, and may contribute to identify theft as well as other fraud. The FTC's guidelines in their effort to safeguard consumer privacy are applicable to the protection of domain name registrants; these safeguards should be appropriately enforced.

Free Speech, Privacy, and Anonymity

On December 10, 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights, which enumerates a list of rights to which all people are entitled. [2] This list includes free speech:

> *ARTICLE 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

It is well understood that the Internet – including chat rooms, email, newsgroups, websites, and domain names – is an unprecedented media through which many people exercise their free speech, including controversial religious and political speech.

The pinnacle of privacy is anonymity.

In the context of the OECD Privacy Guidelines, privacy may be understood as control of your own personal information, control over what others (other people, private organizations, and the government) know about you, and control over how others may use or exploit your personal information. Furthermore, policies and practices that respect privacy aim at minimizing the collection of personally identifiable information. Then intuitively, the starting point of privacy is anonymity, where no personally identifiable information is collected. Compelling the disclosure of personally identifiable information, as current WHOIS policies dictate, directly undermines privacy.

The critical relationship between privacy, anonymity, free speech, and Internet free speech should not be disregarded. [1]

Privacy is critical to free speech. As a simplified explanation, if speakers are compelled to disclose their identity, speakers are reluctant to fully express their speech for fear of persecution. We established that the pinnacle of privacy is anonymity; hence, as a corollary, anonymity is critical for individuals to achieve their fullest ability to exercise free speech.

The United States courts in particular have recognized the importance of Internet free speech and the right of anonymity. [3] The Supreme Court's decision in Reno v. ACLU offers an opinion on why individuals and organizations would want to display material through the World Wide Web:

> *Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. [4]*

For the purposes of political, artistic or controversial speech, the Internet is an unprecedented opportunity to reach a large audience at a relatively small cost. [5]

The one-to-many characteristics of the Internet through which an individual's speech can reach a global audience are further enhanced by the protection of anonymity. [5] In McIntyre v. Ohio Elections Commission, the Supreme Court upheld individuals' ability to distribute anonymous political leaflets and found:

> *Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation; and their ideas from suppression; at the hand of an intolerant society. [6]*

Hence, the Supreme Court upheld the importance of anonymity for individuals to achieve their fullest ability to exercise free speech.

Requiring WHOIS data and then publicly disclosing the data have serious implications on free speech.

Under current WHOIS policies and practices, an individual who wants to create her own website must publicly disclose personal information and cannot remain anonymous. [3] ICANN's Registrar Accreditation Agreement, which requires registrants to supply accurate WHOIS data or otherwise forgo their domain name registration, places an unacceptable burden on the ability of individuals to maintain their anonymity and thus their fullest ability to exercise free speech on the Internet. [1]

Anonymizing proxy servers are not an adequate alternative. [1]

The establishment of an intermediary between the operator of a website and the general public may avoid short-term identification of the actual user of a particular domain name. However, for the most controversial artistic, political and religious speech, it will be difficult for an online speaker to find an intermediary that will offer to have her own identity made public in lieu of the actual speaker. In addition, the third-party licensing provision is unambiguous in stating that the intermediary will be directly liable for use of the domain name by the actual user.

References for this section

[1] Comments of the Public Interest Registry, the not-for-profit corporation that manages the .ORG registry, on the Final Report on Whois Accuracy and Bulk Access of the Whois Task Force of the Generic Names Supporting Organization (hereinafter “PIR Comments on WHOIS”) accessible via http://gnso.icann.org/dnso/dnsocomments/comments-whois/Arc03/pdf00000.pdf.

[2] Marc Rotenberg, The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments 367-394 (EPIC 2002) (“Universal Declaration of Human Rights (1948)”)

[3] Daniel J. Solove and Marc Rotenberg, Information Privacy Law 427-37 (Aspen Publishers2003) (“Anonymity in Cyberspace”).

[4] ACLU v. Reno, 521 U.S. 844, 896-97 (1997).

[5] Letter submitted by EPIC to U.S. House of Representatives Committee on the Judiciary Subcommittee on Courts, the Internet and Intellectual Property, July 12, 2001, http://www.epic.org/privacy/internet/whois_0701.html.

[6] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).

Access and use of the data for legitimate purposes

To be done.

WHOIS as a legal issue

In various countries (including, in particular, the EU's member states), privacy and data protection laws may apply to registrars' WHOIS services and registrars' participation in thick registry WHOIS services. The Task Force is not in a position to give a thorough legal analysis of these aspects, and proposes that the GAC or other relevant multinational bodies be consulted about approaches for designing WHOIS policies in a way which is compatible with such laws.

Policy Options

Principles

Any future WHOIS policy will have to find a proper balance between a number of possibly contradictory principles:

- Registrants' privacy rights must be respected.
- The use of registrants' data must, in general, be transparent to registrants.
- Contracted parties must be able to comply with both applicable law and relevant contracts.
- Legitimate uses of WHOIS data which are crucial to the stability or security of the Internet must continue to be facilitated.

Policy Dimensions

The purpose of this section is to describe a number of possible “dimensions” in which policy might be adjusted, and to discuss possible adjustments.

Differentiating among classes of registrants

Currently, the WHOIS policy in any given gTLD does not differentiate among different classes of registrants: Individual .com registrants, for instance, are handled in the same way as businesses registering in the same TLD. There are first steps to differentiate policies on a TLD level when gTLDs are addressing specific markets: .name offers a WHOIS policy specifically adopted to the intended registrants, individuals, and .biz is the first gTLD since the dissolution of the registry monopoly in which the registry is offering extended search services. However, these policies uniformly apply to all registrants in the given TLD regardless of their status.

The case could be made that WHOIS policy should, in general, distinguish among different classes of registrants – even within a given TLD. In such a scheme, the data set to be published about individual registrants (or non-commercial organizations) could be considerably more restricted than the one to be published about, say, commercial organizations. The data sets could be adjusted to the privacy and transparency needs which would arise with respect to different classes of registrants.

Concerns have been raised about the practicability of this approach: The classification of registrants would have to rely upon information provided by the registrants themselves; enforcing proper self-designation would remain as an unsolved problem. The argument has been made that differentiating WHOIS services by classes of registrants within a single TLD would be practically equivalent to having a minimum set of data elements whose publication would be mandatory, with publication of the remaining data being voluntary.

It has also been observed that individuals, organizations and businesses alike can be engaged in activities for which accountability is necessary.

Similar arguments may be applied on a TLD level, by noting that registrants in special-purpose TLDs may not fulfill relevant eligibility restrictions. However, in this case, the need for transparency may be reduced by the fact that relevant domain names can easily distinguished from sites operating, say, in a name space specifically intended for businesses. As one member of the Task Force wrote: "*The consumer education message is very easy – be careful about buying something from a web site operating in a personal/non-commercial space – they are there because they don't want you to find them.*"

Differentiating among classes of data users and uses

Current policy for query-based WHOIS does, in general, not differentiate among classes of data users, and restrictions on use of data are currently minimal. The situation is different in the RAA's bulk access provisions. Today, there is a specific opt-out provision relating to possible marketing uses of bulk data, and a prohibition of a number of specific direct marketing uses.

If the Task Force's recommended policy changes are adopted, marketing uses of WHOIS data obtained through bulk access will not be permissible any more.

The differentiation among data users could be extended in the bulk WHOIS case: For instance, registrars' bulk access obligations could – unless they are removed entirely – be reduced to making available bulk data only to an extremely limited set of well-identified legitimate data users, for clearly defined purposes.

A tiered access approach for query-based WHOIS could, for example, make some fundamental information available to the general public, and could make more extensive information available to those data users trying to protect their legitimate interests, or exercising legal rights. Law enforcement, in particular, would need to get access to relatively full data. Also, there would be a need for privileged access to WHOIS data for registrars who need to verify the registrant's identity in domain name transfer situations.

This kind of approach poses two key problems:

- The class of a given data user must be verified with reasonable reliability. While this is a relatively easy problem as far as access for accredited registrars is concerned, problems might occur with identifying and verifying law enforcement and other legitimate data users. Some

costs are necessarily associated with this verification function.

- Use restrictions may not actually be enforceable in the query-based case, alone due to the number of data users.

Based on these observations, and based on the concern that complex schemes for verifying classes of data users might not be economically feasible, the following three principles for any kind of tiered access have been proposed:

- A tiered system must be automated;
- a tiered system must be able to automatically handle the bulk of legitimate needs to access whois data;
- registrars must not, in general, be put into the position to judge about the legitimacy of uses.

Differentiating among modes of access

The current policy environment differentiates policies by mode of access: As pointed out above, there are different policies in effect for query-based WHOIS, for bulk access to WHOIS data, and for other modes of access to WHOIS databases which registrars might voluntarily provide to third parties.

Future policy work should explore whether this distinction requires adjustment. For instance, mass queries to port 43 WHOIS can lead to the extraction of significant amounts of WHOIS information without entering into a bulk access agreement; likewise, access to WHOIS data voluntarily provided by registrars, even in bulk, is not currently covered by the RAA's bulk access provisions. Differentiating policies among different modes of (query-based) access may also prove to be a useful tool for implementing a more privacy-friendly WHOIS environment which conforms to the proposed principles given in the end of the previous section. The basic assumption is that certain modes of access to data are inherently unattractive for many illegitimate users:

- Access modes could be designed to generate a small, but measurable cost to data users at certain volumes which exceeds “market prices” for similar address information.
- Technical limitations on the volume of data obtained via Port 43 could make it unattractive for data users interested in using query-based services as a replacement for bulk access.
- Access modes could be designed to inherently generate a relatively reliable audit trail by, e.g., the creation of paper-based contracts between data users and the registrar (registry). Information about the data user could then be made available to the registrant.

An approach based on differentiation among different query-based modes of access could, basically, avoid any direct differentiation among classes of users and uses, and instead grant access to data based on the assumption that certain access modes are, in general, only used by legitimate data users.

Differentiating according to registrants' preferences

One approach which could complement any differentiated access model (either based on a differentiation among data users, access modes, or classes of registrants) is to give registrants some discretion over what data they wish to publish in what way: Registrants could be permitted to make more data elements accessible in any given way than what is mandated by policy.

This approach might contribute to increasing the accountability and transparency at least with respect to good faith registrants who engage in (e.g. commercial) activities which make such transparency and accountability desirable.

WHOIS Issues

(This section is identical to the "issues paper" submitted by the Task Force to the GNSO Council.)

From the beginning of the work of the WHOIS Task Force, a number of discussions and inputs have been received regarding the privacy implications of WHOIS access. In mid 2002, The Task Force chose to separate the treatment of accuracy from access, and recommended privacy be treated separately. Some members of the Task Force do not support this approach and have stated so elsewhere. The majority of the Task Force did Support this approach. Strong commitment to better understanding and addressing the Issues of privacy have been a part of the Task Force discussions. The purpose of this Issues Paper is to identify the issues that have been identified and to briefly discuss them And to present possible policy actions for consideration by the Council.

This document does not address privacy in all WHOIS databases, such as the IP Registry databases, but is focused on the privacy issues in Registrar and Registry WHOIS. The Task Force acknowledges that questions related to privacy in other databases may be addressed by the Council as well.

This list of issues also does not attempt to focus in on the ccTLD WHOIS; the Task Force acknowledges that there are unique issues related to national law which must be taken into account when discussing WHIOS in ccTLD registrations. The Task Force included ccTLDs in its original survey and benefited from the participation and contributions of ccTLD participants. The Task Force would recommend that as further policy work is undertaken, the ccTLD Supporting Organization should be involved in representing the interests of the ccTLDs, or that in the interim until its launch, the ccTLDs could select representatives as delegates to further policy development, as applicable to the ccTLDs.

Issue 1: What is the purpose of WHOIS data collection from registrants, technical and administrative contacts today; what are the uses of the data, today, and who are the various users?

WHOIS data is gathered by the registrars from the registrants [or their agents] as holders of the domain name; as well as technical contact information and administrative contact information. This

data includes a wide range of information that includes name, address, telephone, fax, and email. Other information in WHOIS (Registry level) includes IP addresses for the hosted DNS. The Task Force received comments that understanding the purpose of WHOIS data collection is important to policy development.

The WHOIS Task Force survey identified some of the users of WHOIS data as

- Commercial-Governmental
- Individual
- ISP
- Non-Commercial
- Other
- Registry/Registrar

The purposes of accessing the WHOIS system were also asked of the Survey respondents and included:

- to determine if a specific domain is unregistered/available
- to find out the identify of a person or organization who is responsible for a domain name or web site I have encountered while using the Internet
- To support technical operations of ISPs or network administrators, including tracing sources of spam or denial of service attacks
- To identify the owner of a domain name for consumer protection or intellectual property protection purposes
- To gather names and contact information for marketing purposes
- To support government law enforcement activities (other than intellectual property)
- Other (Please describe)

The survey is merely a snapshot and provides an illustration for some of the reasons to access WHOIS. It has never been presented as a statistically valid survey. During the Task Force's work, other comments were received which documented these general uses of WHOIS. The survey also identified significant concerns with misuses of the WHOIS data for marketing and other purposes that are of concern to users. Comments also included expressed concern by individuals, privacy advocates, and other commenters about access to the WHOIS data when the data is about an individual registrant.

Section 3.3.1 describes the data to be provided in the WHOIS service of the Registrar.

There is a wide difference of opinion regarding the kinds of registrants that make up the major gTLD registrations. Some believe that the majority of registrations are commercial, organizational, or institutional users of a variety of "sizes"; others believe that a large number of individuals are

registered. Some believe that the reason for significant amounts of inaccurate WHOIS data is because individuals are purposely providing erroneous data because they object to having personal data available, for a variety of reasons, while others believe that significant amounts of data from some categories of data have simply "aged". Some believe that many who provide false data are also engaged in fraudulent activities, and are hiding behind the category of "individual registrant".

Before undertaking policy recommendations, an attempt should be made to obtain more information about who registers, and therefore has information in WHOIS, and who uses the data and for what purposes.

A possible policy action would be to establish more clearly a categorization of data users. The exploration should include the importance of providing accurate technical contact information for purposes of security and integrity, based on further advice and consultation from the Stability and Security Advisory Committee. Consideration of relevant policy guidelines from the OECD in both Privacy and Consumer Protection should be taken into account in the development of policy.

Issue 2: There are legitimate needs for public access to registrant data; technical and administrative contact data due to Internet stability issues, consumer protection concerns, policing of trademarks and investigating copyright violations, and ISP/network operators technical concerns. Given these legitimate needs, how can these needs be best met?

Issue 1 lists some, but not all areas that can be examined further as "legitimate" uses of querying the WHOIS database. These are not replicated under this issue but should be considered in full. The Stability and Security Advisory Committee has also provided some comments, which are helpful in this area.

The Task Force has also identified concerns with misuses of WHOIS data. The Task force also has identified that some of its members, and that some in the community believe strongly that absolute rights to anonymity exist. Others in the Task Force believe that there are other considerations, such as engaging in fraud, deception, cyber crime, piracy will present overriding considerations to the right to anonymity.

The Task force notes that the Stability and Security Advisory Committee and some others suggest that there is a critical need for access to registrant contact data that is correct and accurate.

A possible policy action is to explore different ways in which these needs can be met, including 1) continuing the status quo to public access to accurate data in WHOIS 2) exploring tiered access or differentiated/subscriber access 3) providing access without question to law enforcement, but requiring all others to "register" with the registrar. There will be/may be costs for implementing such changes. See Issue 5.

Issue 3: What privacy issues exist in public access to WHOIS: -Via bulk access; -Via port 43? -Via any other arrangement provided by the registrar in bulk access of any kind? -Via public ability to query the database?

The Task Force identified significant concerns related to marketing uses of the WHOIS data, and provided some policy recommendations to begin to deal with changes in bulk access. The Task Force believes that further work is needed to quickly address access to Port 43 that results in data mining and other misuses of the data. Several comments were received by Registrars and other concerned participants regarding such areas. It also suggests that ways that Registrars may make access to the WHOIS data available to third parties under other arrangements or agreements should be examined and suggests possible needs for restrictions to marketing uses that are not consistent with user preferences.

The question regarding public ability to query the WHOIS data base for individual inquiries for all registrants still remains. Some believe that WHOIS should be completely unavailable to public inquiry, while others think that individual access to single queries, or small numbers of queries is acceptable, as long as no data mining or other misuses occur in the query. Some believe that only those registrants who fit a "special" category should be able to rely on anonymity through a third party. Some believe that there are certain "rights" which would allow anyone to remain or operate with anonymity, regardless of whether they are a business, or enterprise, non commercial entity, or individual. Some suggest that it may be possible to allow query as is provided today, with no change. Others suggest that query should be "tiered" with minimal levels of information provided without a "registration" with the registrar.

Applicable Sections of the Registrar and Registry Agreements must be examined in this process for possible change, based on consensus policy.

A possible policy option is that the obligations contained in the RAA's bulk access provisions (3.3.6) could be removed entirely, or eligibility for RAA-mandated bulk access could be limited to certain well-defined, legitimate uses. Access to WHOIS data provided voluntarily by registrars (and use of such data) could be limited by changes to the applicable contracts.

A possible policy option is to maintain the status quo, identify problem areas, and report to Council regarding areas of concern to guide further policy work.

Issue 3a: The current policy environment provides for the possibility that a third party registers a domain name on behalf of the actual registrant, and makes information about the real registrant available under certain circumstances.

It should be explored to what extent such mechanisms are being offered commercially today, and to what extent they contribute to addressing privacy concerns.

Issue 4: For consideration of privacy of the registrant, privacy concerns of organizational, commercial, or institutional registrants who conduct commerce or communication of some kind with the public could be treated differently than privacy concerns of those who are registering as individuals. If so, how would the different categories be defined? How would abuses be addressed so that abuses, after documentation, would lead to a change in status?

Today, there is no distinction between the registrants in the gTLDs, with all registrants asked for the same kinds of information Section 3.3.1-3.3.8) In addition, under Section 3.2, the additional information related to the IP addresses and names of the names servers are also provided by the Registrar to the Registry. It may be appropriate to discuss creating differentiated categories of registrants with different requirements for providing public access to the registration contact information, while still requiring accuracy of information that is provided.

There have been claims of identity theft and other individual user concerns related to the misuse or abuse of WHOIS data which have created individual instances of stalking, or other unpleasant or frightening incidents, that have been described by privacy advocates and civil society activists. Such concerns are very serious and should not be dismissed. Possible approaches could be to undertake an analysis, which would be both expensive, and create serious time delays. On the other hand, it could just be accepted that such risks may exist.

Many believe that by registering a domain name, the registrant is holding himself or herself out to communicate with the public, and that other means of being online, but remaining anonymous exists, such as use of personal web pages with an ISP or other web hoster, or through intermediaries. Others believe that either national law, such as the United States Constitution, or other applicable law, or laws in other countries, guarantee, or require the availability of “anonymous speech” in any medium, based on the choice of the user. The Task Force is, however, not commenting on legal aspects.

As a possible approach for dealing with these concerns, an anonymous or “unlisted” set of information might be appropriate for individuals, with the registrar holding such data, similar to the “unlisted” numbers in the typical telephony white pages. The telephone company holds the correct data, in the event of legal inquiry, or emergency need to contact. In these instances, the telephone company can receive an emergency request to contact from a family member or other entity, and without disclosing the contact number, can contact the individual to ask if they wish to voluntarily contact the inquirer. Law enforcement can also obtain needed information via legal inquiry.

A possible policy action could be to undertake consideration of whether and how to create different categories of registrants in the open gTLDs, and to explore what implications such

decisions would have for restricted gTLDs.

Another possible policy approach would be to maintain the status quo, and ask the ICANN staff to monitor for complaints and problems, and report to the Council.

Issue 5: The current policy environment provides for the possibility that a third party registers a domain name on behalf of the actual registrant, and makes information about the real registrant available under certain circumstances.

It should be explored to what extent such mechanisms are being offered commercially today, and to what extent they contribute to addressing privacy concerns.

Issue 6: If changes in public access to the WHOIS resources are mandated by policy change, will there be costs associated with this change? If so, how should it be funded?

Different views exists about how to deal with funding access to WHOIS overall. The Registrars and Registries have legitimate concerns related to new policy requirements that bring "unfunded" mandates. Users who rely on accurate and accessible WHOIS for a variety of purposes believe that costs of providing basic services should be incorporated in the registration fees and borne by all registrants, as a part of the service to the community and therefore recoverable by the registrars. Some have suggested subscription based services for some categories of users, with others have "free" access for minimal queries. There is yet no well defined agreement on how to fund any changes in WHOIS.

If policy changes are recommended, the full range of implications should be explored, including assessing what the costs would be to registrars to implement differentiated access for different classes of users. Such exploration should include the cost of validation.

Issue 7: Should there be circumstances in which willful provision of inaccurate or incomplete data would not be grounds for possible deletion or other adverse acts? If so, what are those circumstances, and how can it be demonstrated and what safeguards should exist against abuse?

The Task Force heard comments that some may purposely provide inaccurate data or incomplete data as a means to ensure privacy or anonymity.

Based on discussions at the FTC Workshop on Global Fraud, and comments from others,

including the OECD and EC, clearly, some registrants provide inaccurate contact details for reasons that are not about protecting personal privacy for legitimate concerns, but for purposes of defrauding the public. In order to protect those who have legitimate concerns, it is also important to have a mechanism to deal with the "abusers" and to change their status and require correction of data.

If the system were changed, via a policy process, to allow or even encourage the willful provision of inaccurate or incomplete data, corresponding changes in the contractual regime will be needed, coupled with safeguards to deal with abuses.

Issue 8: A broad discussion that ensures input from the GAC, and interested international multi-lateral entities, such as the OECD, the Stability and Security Advisory Committee, the ALAC, the ASO, and the ICANN Board, with the GNSO is needed to further explore the range of issues and questions related to privacy and WHOIS access. Separate discussions and considerations must apply to gTLD WHOIS and ccTLD WHOIS, but where possible, and applicable, ccTLDs representatives and participation should be invited to examine applicable issues, including the development of standards.

Discussions and concerns about privacy and WHOIS are of concern in many other fora, including the GAC and other governmental entities, the ICANN Board, the ALAC, the Stability and Security Advisory Committee, and in the GNSO. WHOIS is important for the stability of the Internet, and the issue of access to the WHOIS data should be treated as a decision that takes into account applicable national law, compliance issues, and requirements for ensuring stability and other legitimate uses. The ccTLDs also have a range of issues related to WHOIS access to data, but national law typically governs them. Since many gTLDS registrars also register in ccTLDs, there is a need to reflect sensitivity to individual requirements. A balanced approach should result from such dialogue that reflects the input of those concerned with privacy, consumer protection, investigation of fraud; and stability of the Internet.

Summary of Comments regarding Privacy Issues and WHOIS:

A balanced approach to considering change is needed, taking into account all perspectives. The consideration of all aspects of the questions and balancing the needs and interests of all may result in: a reaffirmation of the status quo; in a change in who can access WHOIS, how, and under what conditions; in elimination of any kind of marketing uses altogether by limiting contracted, voluntary, or bulk access of any kind to well defined, non marketing purposes; or to no such uses; or ranging from metering of Port 43 to extremely limited access which seems more like query based access with limited inquiries. Other changes could create differentiation of policy among classes of registrants.

The Need for Further Consultation

To be done – or shall we copy this from the "issues paper"?