Issues in WHOIS Privacy

Introduction

The present document is an attempt to give a systematic, high-level summary of perspectives and options with respect to WHOIS policy. It is based on a variety of discussions on the GNSO's WHOIS Task Force.

Background and Perspectives

Privacy Concerns

Privacy concerns about the current WHOIS system roughly come from a number of different directions. Concerns are, in particular, tied to possible harmful consequences of publishing personally identifiable data in WHOIS information, such as identity theft; they are tied to free speech issues such as a right to anonymity; and they are tied to compliance issues in a number of jurisdictions.

Possible Harm Caused by the Publication of WHOIS information

It has been argued that the public availability of WHOIS information may contribute to identity theft, and other fraud. These arguments were, in particular, based on the observation that the US government's FTC has advised consumers not to disclose personal information; if consumers choose to disclose personal information, they have been advised to make sure they know who is collecting that information, and for what purposes.

Free Speech Issues

In the US (and possibly other jurisdictions), a right to anonymous speech is considered to be part of general free speech rights. It has been argued that the current WHOIS provisions – including the "third-party provisions" of the RAA – do not satisfy these needs for anonymous free speech.

Compliance Issues

In a number of jurisdictions (in particular in the European Union), registrar and registry WHOIS services are looked at as a compliance issue with regard to possibly applicable national privacy legislation. The Task Force is not, at this point, commenting on legal issues. Consultation with the GAC and other relevant groups will be needed to fully analyze these questions. However, it has been suggested by some that the OECD's privacy guidelines may be a good starting point for

designing WHOIS provisions which may be compatible with applicable legislation.

Legitimate Uses

It is known that WHOIS access serves a number of legitimate uses. Examples for key uses which are considered legitimate by some parties include:

- handling technical issues;
- policing of trademark and copyright issues;
- law enforcement and consumer protection;
- privacy enforcement.

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.

The Need for Further Consultation

Discussions and concerns about privacy and WHOIS are of concern in many other for a, including the GAC and other governmental entities, the ICANN Board, the Stability and Security Advisory Committee, the At-Large Advisory Committee, and in the GNSO. The ccTLDs themselves 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. 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 national law and requirements for impacting stability and other legitimate uses.

A balanced approach should result from such dialogue which reflects the input of those concerned with privacy, consumer protection, investigation of fraud; stability of the Internet.