

Summary of Public Suggestions on Further Studies of WHOIS including the GAC recommendations of 16 April Updated 10 May 2008

Study submissions have been divided into eight recommended areas, as follows:

- 1. WHOIS misuse studies**
- 2. Compliance with data protection laws and the Registrar Accreditation Agreement**
- 3. Availability of privacy services**
- 4. Demand and motivation for use of privacy services**
- 5. Impact of WHOIS data protection on crime and abuse**
- 6. Proxy registrar compliance with law enforcement and dispute resolution requests**
- 7. WHOIS data accuracy**
- 8. Other proposals recommended by the GAC**

The first two categories of studies examine misuse and legal compliance problems that motivate proposals to require WHOIS data protections. The third category examines the availability of privacy services in the marketplace to understand the extent to which services that provide WHOIS data protections are already available at a reasonable cost. The fourth category examines the demand and motivation for use of privacy services to determine the fraction of registrants who would legitimately benefit from them and the extent to which they are currently being used for illegitimate purposes. The fifth category examines the impact of WHOIS data protection on reported crime and abuse incidents. The sixth category examines whether procedures for revealing the identity of an underlying registrant or relaying communications to registrants effectively meet the needs of law enforcement and dispute resolution processes. The seventh category examines questions of WHOIS data accuracy. Finally, the last category includes several study areas recommended by the GAC that do not fall into the previous identified groupings.

This summary report describes each study proposal in the left column, and the rationale for conducting such a study, where provided, in the right column.

1. WHOIS misuse studies

Five study submissions (submissions #1, #14, #15 and #21 and GAC bullet #2) suggest that ICANN study misuse of WHOIS data to determine the connection, if any, between WHOIS and illegal activities. These studies will help establish the extent and nature of problems caused by unprotected WHOIS data.

| | |
|--|---|
| <p>Study Submission # 1: 1) Gather data on WHOIS misuse from consumer protection bureaus and other entities who maintain data on misuse incidents reported by registrants and 2) survey a random sample of registrants in each gTLD and selected ccTLDs.</p> | <p>If a significant number of misuse cases involve receipt of unwanted email (spam), ICANN could modify its policies to reduce automated harvesting of email addresses from WHOIS. For instance, ICANN could require that registrars use data protection measures (e.g. captcha) on all WHOIS inquiry services. ICANN might also modify policies governing entities and processes for bulk retrieval of WHOIS data.</p> |
| <p>Study Submission # 14: Create a set of new email addresses, use half of them to register domain names, and monitor all for spam for 90 days to determine how much WHOIS information contributes to spam.</p> | <p>The results would speak to the validity of the argument that modifications to WHOIS would be useful in deterring spam and other such illegal or undesirable activities.</p> |
| <p>Study Submission # 15: Create a set of new email addresses, use them to register new domain names at registrars that allow and disallow port 43 WHOIS queries, and monitor all for spam to determine the extent to which port 43 WHOIS queries contribute to spam.</p> | <p>If most use of WHOIS to facilitate illegal or undesirable activities is traceable to data mining over port 43, perhaps a proposal that focuses on controlling the means of access to WHOIS (such as by allowing a combination of web-based access, providing alternate solutions for legitimate current uses of port 43, and authenticated port 43 access), rather than removing particular fields of data from availability, could be effective in controlling data mining, spam, or other harms, while preserving substantially unrestricted access for legitimate uses.</p> |
| <p>Study Submission # 21: Survey registrars and human rights organizations to determine how WHOIS is being used in ways that seem to have no bearing on the security and stability of the DNS.</p> | <p>This study would provide data for assessing uses of the public WHOIS data unrelated to DNS. Should abuses be found, a full report would provide a basis for changes to WHOIS that would provide WHOIS data for DNS purposes, without providing it for uses (and abuses) unrelated to the DNS. This data would provide a well-informed basis for offering changes to WHOIS policies.</p> |
| <p>GAC bullet #2: the types and extent of misuses of WHOIS data and the harm caused by each type of misuse, including economic, use of WHOIS data in SPAM generation, abuse of personal data, loss of reputation or</p> | |

| | |
|--|--|
| identity theft, security costs and loss of data. | |
|--|--|

Study submission numbers 1 and 21 propose to survey registrars and other parties who may keep records of misuse incidents. 1 also proposes a survey of registrants. These proposed studies may shed some light on the extent and type of misuse of WHOIS data. However, it will be difficult to gather representative data as not all cases of abuse are reported. In addition, it is not always possible to confirm that misused data was obtained from WHOIS, as this information may be available from other sources. A registrant survey is likely to receive disproportionate responses from registrants who believe their WHOIS information has been abused. Nonetheless, the above studies may result in useful qualitative data about the nature of misuse and provide a rough quantitative estimate of the extent of misuse. Surveying those who already keep track of abuse incidents is likely to be a relatively low-cost approach. The registrant study is likely to be more expensive if done on a large scale, and seems less likely to result in useful data.

Study submission numbers 14 and 15 focus on spam and propose studies in which new email addresses are created and used to register domains to determine how much WHOIS information contributes to spam. #15 compares the amount of spam received as a result of registering a domain at registrars that allow and prohibit port 43 WHOIS queries. These studies should result in fairly accurate quantitative data. However, #14 is quite similar to the October 2007 SSAC study “Is the WHOIS service a source for email addresses for spammers?” and would not likely contribute new information. If port 43 queries are of interest from a policy perspective, study #15 should provide reliable data to inform that discussion.

2. Compliance with data protection laws and Registrar Accreditation Agreement

Three study submissions (#16, #22, #23) suggest studies of data protection laws and how they relate to ICANN and ccTLD policies for WHOIS and other personal domain name registration data. The results of these studies would provide insights into whether current policies and practices comply with national data protection laws. Study #24 proposes to determine whether registrars’ registration agreements comply with the Registrar Accreditation Agreement. The results of these studies may suggest the need for policy changes or better enforcement measures. These studies involve a legal review and analysis of publicly available documents, and possibly a questionnaire distributed to top ccTLDs. Data collection for these studies should be relatively inexpensive but requires willingness on the part of ccTLD operators to participate. Analysis will require legal expertise.

| | |
|---|--|
| Study Submission # 16: Conduct legal analysis under the laws of a variety of jurisdictions of the terms of various registrars’ registration agreements concerning data collection and disclosure and their process for | It would identify whether registrants are validly consenting in a verifiable and enforceable manner to the submission of their personal information in WHOIS records (or whether their consent could be valid if modifications were made to registrars’ processes), thus suggesting that additional measures either are, or are not, necessary to bring WHOIS services in conformance with the requirements of |
|---|--|

| | |
|---|--|
| collecting such data and obtaining consent. | national privacy laws. |
| Study Submission # 22: Survey top 25-30 ccTLDs to determine the extent to which ccTLD WHOIS policies reflect national data protection laws and priorities. | If the hypothesis is proven, then the data protection aspects of numerous ccTLDs policies should be compiled, analyzed and studied. To the extent that there are overlapping provisions or principles, they serve to guide ICANN staff and the GNSO in revising and redrafting the long-standing WHOIS policies of ICANN. |
| Study Submission # 23: Conduct a legal comparison of national data protection laws to determine legal requirements relevant to the protection of registrant information. | The study results can provide considerable guidance to the GNSO if, for example, it is found that entire regions of the world have data protection laws. In that case, aspects of these laws should inform and guide changes and improvements to ICANN's WHOIS policies. The Constituencies can then review changes to WHOIS, and changes can be adopted by consensus policy. |
| Study Submission # 24: Obtain a representative sample of registrars' terms and conditions to determine what percentage of sampled registrars is appropriately obtaining agreement to all of the terms required under Section 3.7.7 of the RAA. | This study would identify whether registrars are complying with the RAA. It would also identify whether problems with WHOIS currently require policy changes or better enforcement of existing agreements. It would also act as a barometer concerning whether registrars and their affiliates could be relied on to enter into required agreements with registrants and enhanced obligations, should a more restrictive WHOIS system such as OPoC be implemented where registrars and their affiliates would be required to obtain the registrants' consent to act as the custodian of information and relay communications in a more robust way. |
| GAC recommendation #12: Since gTLD registries and registrars conduct business globally, which laws in which jurisdiction appropriately apply to their transactions and in particular to their WHOIS contractual obligations? | This is similar to some of the previous study submissions, but the previous proposals are more narrowly focused on data protection laws. |
| GAC recommendation #13: What are the legal jurisdictional issues raised by gTLD registries and registrars that adhere to local law applicable to domain name registrations and | This is also similar to some of the previous study submissions, but the previous proposals are more narrowly focused on data protection laws. |

| | |
|---|---|
| WHOIS requirements, but may then be in contravention to other legal jurisdictions where they conduct business? | |
| GAC recommendation #14: May a gTLD domain name registrant who is a legal resident of one country apply for a domain name in another and claim to be under the legal jurisdiction of the latter and not the former? | This is also similar to some of the previous study submissions, but the previous proposals are more narrowly focused on data protection laws. |
| GAC recommendation #15: How can conflicts of laws be resolved in a global domain name space? | This is also similar to some of the previous study submissions, but the previous proposals are more narrowly focused on data protection laws. |

3. Availability of privacy services

Proposals #2 and #5 would study the current availability of privacy services, determine their costs and extent of use, and correlate use with cost and other features.

| | |
|--|---|
| Study Submission # 2: 1) Gather data on types of privacy services offered through manual review of websites offering registration services and survey of registrars and 2) attempt to correlate service characteristics (cost and features) with the relative share of eligible registrants who choose to use a given privacy protection service. | An affirmation of the hypothesis would not necessarily drive changes to WHOIS policy. However, ICANN could undertake communications efforts to educate registrants about their options in shielding personal data. ICANN also could undertake policy development to standardize the minimum features required of proxy services. If the analysis finds that registrants have only one privacy protection option available, ICANN could undertake policy development to increase availability and competition among registrars and other providers of privacy protection services. |
| Study Submission # 5: Study whether resellers and registrars offer privacy services to differentiate themselves from others, and, if so, whether this is a factor that encourages competition and whether it is available at no | The study could prove that removing the WHOIS as it is - or building in an element of privacy at the registry level - will remove privacy services as a differentiator of service and thus reduce competition in this industry. |

| | |
|---|---------------------------------|
| charge. | |
| GAC recommendation #7: What is the historical trend and current percentage of the registrars' and their affiliates' proxy and privacy registrations in relation to the total number of domain name registrations in gTLDs? | Relates to Study submission #2. |
| GAC recommendation #8: What is the percentage of registrars and all affiliates that offer proxy or privacy registrations? | Relates to Study submission #2. |

Determining the availability, cost and features of privacy services can be done easily through a survey of the publicly available information on the registrars' web sites, and would provide useful data on whether such services are readily available in the market at little or no cost to consumers. To measure the extent of use and correlate use with cost and other features will require additional data collection, probably through registrar questionnaires. This would provide information about consumer interest in privacy services and willingness to pay for these services. It is unclear how these results will shed light on the question of whether current WHOIS policies encourage competition, or whether these policies ultimately benefit consumers.

4. Demand and motivation for use of privacy services

Proposals #17, #18, and #19 explore the demand and motivation for use of WHOIS privacy services. They assume that individual registrants who are natural persons have the greatest demand for using privacy services and that legal entities may not have a legitimate interest in these services, and may even use these services for illegitimate activities. Thus, proposal 19 proposes to determine the fraction of registrants who are natural persons across all domains. Proposal 18 focuses on determining the fraction of proxy-registered domains that appear to be registered by natural persons through an examination of their websites. Proposal 17 suggests an online questionnaire be administered to registrants who use proxy services to determine their motivation for using those services.

| | |
|--|---|
| Study Submission # 17: Survey proxy/privacy service registrants to determine their reasons for using a proxy service. | The study may reveal that a large portion of registrants have legitimate privacy concerns and are not engaged in illegitimate activity. |
|--|---|

| | |
|---|---|
| | |
| Study Submission # 18: Sample proxy service registrants and review their sites to determine what percentage are likely individual registrants concerned about their privacy. | If it is shown that the majority of registrations by proxy are used to hide the owner of a domain name that is used for a commercial enterprise, then the policy arguments for privacy are diminished, as compared with the use of proxy registrations by individuals for non-commercial purposes. |
| | |
| Study Submission # 19: 1) Sample WHOIS records to determine what percentage of registrations are owned by natural persons, legal persons, and proxy services, and 2) survey registrars to gather similar information as well as information about requests to reveal the identity of the registrant. | The study results would aid in showing whether there actually exists a relevant, legitimate interest in services (or ICANN policies) that shield the identity of the actual domain owner. If there is little relevant interest in such services, ICANN might consider whether proxy services and similar services should be abandoned or proxy registrations limited to those with legitimate interest. |
| | |
| GAC recommendation #9: What are the relative percentages of legal persons and natural persons that are gTLD registrants that also utilize proxy or privacy services? | This is related to study suggestion numbers 18 and 19. |
| | |
| GAC recommendation #10: What are the relative percentages of domain names used for commercial versus non-commercial purposes that are registered using proxy or privacy services? | This is also related to study suggestion numbers 18 and 19. |

These studies appear to be getting at two distinct questions: What fraction of registrants have legitimate interests in privacy services? What fraction of the registrants who currently use privacy services are using them for illegitimate purposes? Suggestions 18 and 19 are reasonable approaches to estimating the fraction of natural persons among samples of registrants. However, it is not clear that only natural persons have a legitimate interest in privacy services, as businesses may also wish to use these services—for example to reduce spam on corporate networks or to protect the privacy of their employees. A better metric may be needed to determine which registrants are using proxy registrations for illegitimate purposes. The online survey of registrants proposed in suggestion 17 seems unlikely to result in accurate self-reported data.

5. Impact of WHOIS data protection on crime and abuse

Studies #6 and #13 propose to examine the impact of WHOIS data protection on crime and abuse. While the previous category of studies proposed to gather data to provide insights into the fraction of proxy registrants who might be using data protection services for illegitimate purposes, proposals in this category study reported abuse incidents. Study 6 proposes to compare crime/abuse levels across ccTLDs with more restrictive WHOIS access than ICANN’s gTLDs. Study 13 proposes to determine whether phishers are using privacy services and, if so, how this impacts shut-down times for phishing sites.

| | |
|---|--|
| <p>Study Submission # 6: Study whether more restrictive WHOIS data policies lead to more crime and abuse by comparing crime/abuse levels on a percentage basis across two or more ccTLDs with different and/or more restrictive WHOIS access than ICANN's gTLDs.</p> | <p>Some legitimate groups support the status quo (open, unrestricted access to all WHOIS data) because they fear that any restrictions on access to WHOIS data will produce increases in cyber-crime and insecurity. If experience proves that those fears are unfounded, then it could produce broader consensus on policies to shield some information of natural persons.</p> |
| <p>Study Submission # 13: Conduct analysis of APWG phishing web site data to determine whether phishing web sites tend to be hosted on private/proxy domains and to understand how shut down times of phishing sites are impacted by proxy/private WHOIS registrations.</p> | <p>We would like to find a balance between maintaining the privacy of individuals while maintaining the security of the internet from phishers. Therefore, our hope is that if there has been an increase of the use of proxy and privacy services in WHOIS registrations that there could be a policy adopted that allows certain organizations (like those affiliated with the APWG and others) to access the data behind records that use private and proxy registrations. Safeguards may be needed to prevent abuse of this data access, but this study may help justify the formation of policy that gives immediate access to this information in certain circumstances.</p> |
| <p>GAC recommendation # 11: What is the percentage of domain names registered using proxy or privacy services that have been associated with fraud or other illegal activity versus the percentage of domain names not using such services that have been associated with fraud or illegal activity?</p> | <p>This is related to study submission numbers 6 and 13.</p> |
| | |

| | |
|--|---|
| GAC recommendation #1: To what extent are the legitimate uses of gTLD WHOIS data curtailed or prevented by use of proxy or privacy registration services? | This is relevant to the previously listed study submissions because access to WHOIS data is one of the legitimate uses we would like to protect, but there may be other legitimate uses not mentioned by previous proposals. |
| | |
| GAC recommendation #2: What is the economic impact of restrictions on some or all of the legitimate uses of WHOIS? | This is also relevant to the previously listed study submissions because access to WHOIS data is one of the legitimate uses we would like to protect, but there may be other legitimate uses not mentioned by previous proposals. |

These studies seem like reasonable approaches to studying the impact of WHOIS data protection on crime and abuse. APWG has volunteered use of their phishing data set for study #13.

6. Proxy registrar compliance with law enforcement and dispute resolution requests

Three proposals (#3, #20, and Metalitz) suggest studies that will determine whether proxy registrar procedures for revealing the identity of an underlying registrant or relaying communications to registrants effectively meet the needs of law enforcement and dispute resolution processes. These suggestions propose to gather data by reviewing stated policies, collecting data from requesting parties, and submitting inquiries and measuring response time. Study 13 in the previous category also includes a similar component.

Before deciding whether or not to conduct a study in which requests are submitted to measure response time, it would be useful to first determine what data on response time is available from requesting parties. A small study might be useful to independently verify reports from requesting parties. A larger study might be needed if little or no data is available from requesting parties.

A related study suggestion, #12, proposes to inventory law enforcement requirements and determine how to balance them with individual privacy needs. Such a requirements analysis, combined with results of the other studies in this category, would provide insights into whether law enforcement needs are currently being met.

| | |
|---|---|
| Study Submission # 3: 1) Review stated policies of registrars and privacy protection services to determine whether they comply with the RAA and 2) determine actual compliance through a) reports from requesting parties and consumer protection agencies and b) submitting | If the hypothesis were verified, ICANN should improve its contractual compliance efforts for registrars offering proxy services. ICANN’s response should be proportional to the quantity of registrars and affected registrants where compliance was found to be deficient. If non-compliance is confined to a small number of registrars, increased contract enforcement efforts could be limited and targeted. On the other hand, a widespread lack of compliance |
|---|---|

| | |
|--|--|
| properly constructed inquiries and measuring response time. | might indicate that ICANN should amend the RAA to increase penalties for non-compliance. |
| Study Submission # 20: Survey proxy registrars, brand owners and law enforcement officials and/or conduct a study to determine timeliness of proxy services in relaying communications to registrants and/or revealing the identity of underlying registrants per RAA 3.7.7.3. | Data collected could inform and quantify the need for additional regulation of the responsibilities of proxy services to relay communications and/or to reveal registrant contact information upon receiving reasonable evidence of actionable harm. |
| Metalitz Comment: Collect data on UDRP cases brought against registrants who used proxy or private registration services to determine the extent to which a registrant's use of a proxy/private registration service reduced the registrant's ability to contest a UDRP proceeding. | This data would provide a quantitative basis for determining whether any changes were needed in current policies regarding the operation of proxy/private registration services, or regarding the UDRP, in order to protect the interests of registrants, or to improve WHOIS data accuracy. |
| Study Submission # 12: Inventory privacy requirements and law enforcement requirements related to WHOIS. | The better the data in WHOIS is and a proportional access is assured the less the need for strict rules for access will be. |

7. WHOIS data accuracy

Two proposals (suggestions #8 and #11) suggest that ICANN study certain questions of WHOIS data accuracy. These proposals are orthogonal to questions about the extent to which WHOIS data should be protected. In conducting these studies, researchers would first need to establish objective criteria to determine whether records have been falsified or whether accuracy and readability have been impaired. As a large sample size is needed, the expense of these studies is dependent on the extent to which the analysis can be automated.

| | |
|---|--|
| Study Submission # 8: Sample WHOIS data from domains at several registrars and check | Registrars which chronically violate ICANN policies in regards to WHOIS accuracy could have their accreditation revoked. |
|---|--|

| | |
|--|--|
| records for valid combinations of address and phone information to determine whether registrars are tolerating systematic abuse of WHOIS records. | |
| Study Submission # 11: Examine whether IDN (non-ASCII) characters in TLDs will impair the accuracy and readability of WHOIS records displaying the domain name, email address, and name server addresses. | If analysis supports this hypothesis, ICANN should undertake policy development to amend requirements for WHOIS data collection and display. |

8. Other GAC recommendations –

These do not fall into the previous identified groupings. The first bullet, and recommendations 5 and 6 propose to gather general statistics about domain name registrants and WHOIS users. GAC recommendation #3 is also not covered by previous proposals.

| | |
|--|--|
| GAC bullet #1: compile data that provides a documented evidence base regarding the amount and source of traffic accessing WHOIS servers and the types and numbers of different groups of users and what those users are using WHOIS data for. | |
| GAC Recommendation # 5: What is the percentage of domain name registrants who are natural persons versus legal persons (or entities)? | |
| GAC Recommendation # 6: What is the percentage of domain name registrations that are registered for and/or are used for commercial purposes versus those registered | |

| | |
|---|--|
| for non-commercial or personal use? If possible, the data should be broken down by geographic (e.g. by continent) locations. | |
| GAC Recommendation #3: Are technical measures available that could effectively curtail misuse of data published on WHOIS databases while preserving legitimate use and open access to the databases? | |

Out of scope proposals:

Three public submissions (submissions #4, #7 and #9) appear out of scope.

Study Submission # 4: Study best approach to offering transport layer security for WHOIS queries.

Study Submission # 7: Find a way to stop domain name thieves or protect domain owners from unscrupulous providers.

Study Submission # 9: Survey webmasters to determine whether they have observed the top 10 registrars locking domains after a domain name search.