ICANN

The Internet Corporation for Assigned Names and Numbers

**Report for the GNSO Council on WHOIS Privacy and Proxy Abuse studies**

Prepared by Liz Gasster
October 5, 2010

## Background

The GNSO Council has concluded that a comprehensive, objective and quantifiable understanding of key factual issues regarding the gTLD WHOIS system would benefit future GNSO policy development efforts. In March 2009, the GNSO Council asked ICANN staff to research the feasibility and cost to study several high priority aspects of WHOIS. Staff categorized these studies into four areas that could be researched independently, and solicited bids using an RFP approach to help determine costs and feasibilities. This report provides staff analysis for one study area: **WHOIS Privacy and Proxy Abuse**.

## Summary of staff approach

To assess the feasibility and cost of proposed WHOIS studies, Terms of Reference (ToR) have been drafted to define each study area at the level of detail required for research organizations to propose tasks, schedules, and fees to execute proposed studies. The GNSO community provided input on draft ToRs to ensure alignment between study definitions and key factual issues regarding WHOIS which they believed would benefit future policy development efforts.

Two RFPs for **WHOIS Misuse** and **WHOIS Registrant Identification** studies were posted in late 2009 and assessed in March 2010. On 8-Sep-2010, the GNSO Council resolved to proceed with WHOIS Misuse studies. Related documentation can be found here:

http://www.icann.org/en/announcements/announcement-28sep09-en.htm
http://www.icann.org/en/announcements/announcement-23oct09-en.htm
http://gnso.icann.org/issues/WHOIS/WHOIS-studies-report-for-gnso-23mar10-en.pdf

A third RFP defining **WHOIS Privacy and Proxy Abuse** studies was posted on 18-May-2010. Interested bidders were given 60 days to respond, followed by 30 days to clarify proposal details needed to complete assessment. That RFP, analyzed in this report, can be found here:

http://www.icann.org/en/announcements/announcement-2-18may10-en.htm

A fourth RFP defining **WHOIS Privacy/Proxy Relay & Reveal** studies was just posted here:

http://www.icann.org/en/announcements/announcement-29sep10-en.htm

**Staff Analysis of WHOIS Privacy and Proxy Abuse Studies**
In the analysis that follows, staff considers the merits and limitations of conducting proposed WHOIS Privacy and Proxy Abuse studies, based what we have learned to date from bidders. This report also provides our initial assessment of those bids, based on objective criteria (see Annex).

**Overview:** These studies are intended to help the ICANN community determine the extent to which Proxy and Privacy services are abused during illegal or harmful Internet communication. Specifically, researchers would attempt to prove/disprove the following hypothesis:

*A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.*

This hypothesis would be tested by studying a representative sample of gTLD domains allegedly involved in various kinds of illegal or harmful Internet communications documented by organizations that routinely track, investigate, and/or remediate such incidents. To measure the relative frequency of Privacy/Proxy abuse, these domain users ("bad actors") would be divvied into those that can be reached directly using WHOIS data and those that must be contacted via a Privacy/Proxy service.

Because the nature and duration of illegal/harmful Internet activities varies, two sampling methods were proposed in the ToR: Live-Feed Monitoring for incidents typically reported in real-time (e.g., spam, phishing) and Offline Third-Party Recording (e.g., trademark infringement, cybersquatting) where live-feeds do not exist but incident reports might be obtained from study participants instead. To help bidders determine study scope, the ToR included a broad "starter list" of activity types and possible input sources, to be finalized during the first phase of study. Once gathered, this alleged "bad actor" domain sample would be classified and filtered to measure the relative frequency of Privacy/Proxy registrations, broken down by activity type.

**RFP Responses At-A-Glance:**
We received three bids in response to this RFP. Applying the assessment criteria defined in the Annex, staff found two bids to be viable contenders for performing this study. After requesting bid clarifications, one RFP response emerged as superior.

Both top-ranking responses were aligned with study goals, considered possible input sources, addressed potential challenges, and covered comparable subsets of the illegal/harmful activities listed in the ToR. Both responses proposed balanced, qualified teams that would bring unique strengths to this project. One bid demonstrated deeper understanding of cybercrime and appears more likely to produce respectable results that could contribute meaningfully to WHOIS policy debate.

Costs to perform these studies ranged from $50K to $200K, reflecting very different proposed sample sources, sizes, and study periods (5 to 18 months). The superior bid proposed a 5 month study at a cost of approximately $150,000. However, this bid's proposed timeline did not include necessary preparatory efforts that would likely result in longer total elapsed time to complete the study. If the Council opts to conduct this study, we would need to revisit the timeframe and final costs to complete the study.

The superior RFP response surpassed all assessment thresholds and demonstrated a solid grasp on the task at hand. This proposal would apply a multi-national team, drawn from three top-tier research universities, lead by a highly-regarded research facility. Team members would apply diverse cybercrime expertise and use feasible methods to conduct a significant portion of this study at a competitive price.

However, no response (including the superior bid) covered the entire range of illegal/harmful activities identified by the ToR. All focused on Live-Feed Monitoring as a preferred method of sampling. Only one bid included Offline Third-Party Reports, but warned that obtaining sufficient participation would be problematic. As a result, all responses would measure the frequency of Privacy/Proxy registrations across a narrower set of incident types, obtained from sources that bidders identified would supply the most plentiful and relevant samples.

This narrower scope could diminish WHOIS policy contributions by failing to address the concerns of a few constituencies. However, this may be offset by deeper analysis of sampled domains. One bid proposed comparing the rate of Privacy/Proxy registrations with this sample to the rate at which other methods are used to obscure perpetrator identity, such as falsifying WHOIS data, exploiting compromised machines, and free web hosting. This approach could provide useful context, helping the ICANN community assess not just the relative frequency, but the significance of Privacy/Proxy abuse.

**Staff Recommendations about Privacy/Proxy Abuse Studies, based on RFP responses:**
The key challenge for this study appears to be obtaining statistically-meaningful data that is relevant to the study's hypothesis. Based on responses, researchers can easily study representative samples of some illegal/harmful activities, including spam, phishing, malware, software piracy, counterfeit merchandise, money laundering, child pornography, and cyber/typo squatting.

However, researchers questioned the relevance of including on-line stalking, DoS attacks, DNS poisoning, media piracy, advanced fee fraud, and IP or identity thefts beyond activities covered more specifically above. For example:

- IP-sourced activities like DoS attacks and DNS cache poisoning tend to be investigated using contact data obtained from Regional Internet Registries (e.g., RIPE, ARIN) instead of WHOIS,

- Media piracy sites tend to be investigated by contacting site hosting providers rather than WHOIS-identified domain users, and

- Reply-To addresses found in Advanced Fee Fraud email usually point to free webmail accounts that are not typically investigated using WHOIS.

In short, studying these activities would not help prove or disprove this study's hypothesis because real-world investigations would not likely consult WHOIS data.

Based on responses, it appears that sufficiently diverse data can be obtained by Live-Feed Monitoring alone. While Third-Party Reporting might broaden the scope of sampled data, it would do so only slightly, while adding hard-to-meet external dependencies, significant complexity, and unclear value.

Obtaining timely WHOIS data and classifying it does not appear to present any insoluble barriers. The exception may be filtering out "false positives." This study would analyze WHOIS data associated with *all* alleged bad actors (proven or otherwise). No bidder suggested how to reliably weed out low-probability cases – especially for Privacy/Proxy domains where registrant/licensee contact is more difficult. Including false positives could skew results in either direction, reducing their value to policy debate.

To better inform policy, this study must determine not just the frequency of Privacy/Proxy registrations, but that rate's significance. There appear to be several promising ways to accomplish this:

- To compare the rate of Privacy/Proxy registrations to the rate of alleged bad actor WHOIS data that is simply not usable, the accuracy of sampled WHOIS data could be evaluated.

- To assess the rate at which alleged bad actors are associated with compromised machines or used without the registrant's knowledge, registrant contact could be attempted. Although contact is unlikely for Privacy/Proxy registrations, this could still add useful context at little additional cost.

- To provide a control sample against which to compare WHOIS data accuracy and Privacy/Proxy registration rates, a randomly-selected set of domain names for lawful websites could be analyzed, chosen to mirror sites involved in illegal/harmful activities to be studied.

In summary, the benefit of running this study is to supply empirical data on how often alleged bad actors obscure their identity using several common methods, including (but not limited to) Privacy/Proxy registration. However, findings produced by this study may not represent some longer-lived illegal/harmful activities, and they appear unlikely to reliably differentiate between alleged and confirmed bad actors. Even so, if Privacy/Proxy use is high among bad actors, as compared to a control sample or to other methods of obfuscation, policy changes may be warranted to deter this abuse.

**Suggested Next Steps**

This report is one of several aimed at responding to the GNSO Council’s request to determine the costs and feasibility to conduct various WHOIS studies. Staff recommends that the Council review this information when considering whether to approve additional WHOIS studies.

Staff is available to answer questions about this report and to provide additional information as requested.  We will continue working on the fourth proposed WHOIS studies RFP, and will provide regular updates and further information as it becomes available.

**Annex – WHOIS Study RFP Assessment Criteria**

To help determine WHOIS Study cost and feasibility, an RFP approach was used to solicit proposals from independent researchers. This describes how those proposals were assessed.

**Proposal Assessment Grid**

| | | | |
|---|---|---|---|
| Request for Proposals: | | | |
| Bidder: | | | |
| Name of proposal evaluator: | | | |
| | Max Score | Evaluators' Score | Minimum Threshold |
| Understanding of the assignment (total) | 30 | | 20 |
| - Understanding of the Terms of Reference | 15 | | |
| - Alignment with study hypothesis and goals | 15 | | |
| Qualifications of bidder (total) | 40 | | 25 |
| - Previous similar research activities | 10 | | |
| - Suitability of proposed CVs | 10 | | |
| - Previous experience with DNS and WHOIS services | 10 | | |
| - Other skills required or given special merit by the RFP | 10 | | |
| Proposed methodology and tools (total) | 55 | | 30 |
| - Suitability of timetable | 10 | | |
| - Work organization and methodological approach | 15 | | |
| - Suitability of proposed data gathering tools | 15 | | |
| - Suitability of proposed data analysis / validation methods | 15 | | |
| Financial offer (total) | 15 | | 10 |
| - Effort justified and consistent with proposed methodology | 10 | | |
| - Overall value of money | 5 | | |
| **Overall Score** | **140** | | **85** |

**Proposal Assessment Process**

1. Assessment of proposals will be carried out by a review panel composed of ICANN staff.
2. Evaluators will read all proposals received and then score each proposal using the above grid.
3. The panel leader will produce a final assessment grid for each proposal received by averaging the individual evaluator scores attributed to each bid, under each criteria of assessment.
4. Proposals failing to obtain – in the final assessment grid – the minimum thresholds for all four main criteria of assessment will not be considered for contract awarding.
5. The final assessment grid for the two bidders scoring the highest marks, accompanied by a list of verified references, will be presented to ICANN management for final bidder selection.

**Proposal Assessment Criteria**

1. **Understanding of the Assignment:** This criterion measures how well each bidder understood the two key elements making up this assignment, namely:

    - Understanding of the Terms of Reference: Does the proposal's scope and approach reveal an accurate understanding of the ToR? Does it contain all elements required by the RFP? Does it demonstrate an understanding of the subject matter and the work involved?

    - Alignment with study hypothesis and goals: How well does the proposal align with study hypothesis and goals identified by the ICANN community and stated in the ToR? (independent of the method(s) proposed to prove/disprove that hypothesis)

2. **Qualification of bidder**: This criterion measures how suitable the bidder is to conduct the study, both as a bidding organization and as a team of individuals that are to perform the work:

    - Previous similar research activities: Has the bidding organization conducted Internet crime experiments or large-scale user surveys for other organizations or ICANN? Zero points for no prior activities; otherwise, score should reflect frequency of activities and relevance to task at hand. Credible peer-reviewed research is given greater weight.

    - Suitability of proposed CVs: Do the individual team members have the background and expertise needed to carry out the work? Do CV's complement each other in order to cover all required skills and areas of expertise? Has the team worked together well before?

    - Previous experience with DNS and WHOIS services: Does the proposed team have prior research experience with DNS in general and WHOIS in particular? How well is the team likely to already understand the parties and processes involved in DNS, and the issues related to domain name registration, WHOIS access, and Privacy/Proxy services?

    - Other skills required or given special merit: Does the proposed team have any special skills required by the RFP (e.g., ability to read/speak non-English text) or any attributes cited by RFP as deserving special merit? Would the bidder's reputation bring added benefits to the ICANN community or speed progress on WHOIS-related studies? Are there potential conflicts of interest (e.g., bidder has vested interest in study results)?

3. **Proposed methodology and tools:** This criterion measures how well the bidder's approach reflects rigorous consideration of one or more studies outlined by the ToR, and whether the proposed methodology and tools appear to be suitable and feasible.

    - Suitability of timetable: Does the schedule included in the response reflect the proposed approach and appear to be credible and implementable? Are there any critical activities proposed that cannot realistically be accomplished?

    - Work organization and methodological approach: Is the work logically structured in clearly identified phases? Is the scope of each phase clearly described? Are external constraints and dependencies clearly identified and taken into consideration? Have important issues been overlooked? Are all necessary quantitative and qualitative elements of analysis addressed by the bidder's proposed methodology?

    - Suitability of proposed data gathering tools: Are the proposed sample generation and data gathering approaches consistent with the overall direction given the ToR? Are they consistent with the bidder's proposed methodology? Does the proposal suggest creative data gathering approaches that would help the study better evaluate its stated hypothesis? Does the proposal take into consideration necessary interaction with other parties (e.g., users to be surveyed, dependencies to be contacted)?

    - Suitability of proposed data analysis / validation methods: Are the proposed data analysis methods suitable to aggregate, interpret, and weight study findings? Would those findings address the stated study hypothesis? Are validation mechanisms or limitations of findings and conclusions foreseen and described? Does the proposal anticipate the need to communicate and review preliminary findings with the ICANN community?

4. **Financial offer:** This criterion measures two elements of the bidder's financial offer:

    - Effort is justified and consistent with proposed methodology: Do the projected efforts appear to be a realistic estimate of the work required to execute the proposed study? Have any necessary expenses been omitted? Have staffing requirements and efforts been described and justified in sufficient detail to enable review?

    - Overall value of money: Evaluators are invited subjectively rank proposals on their value for the money. The proposal representing the best value for the money should be scored a **5**, while that representing the worst value for the money should be scored **0**. Other proposals should receive intermediate scores.