At-Large Study on Whois Privacy & Proxy Service Abuse Workspace

Comment Close Date	Statement Name	Status	Assignee (s) and RALO(s)	Call for Comments	Call for Comments Close	Vote Announcement	Vote Open	Vote Reminder	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
22.10.2013	Study on Whois Privacy & Proxy Service Abuse	Adopted 13Y, 0N, 0A	• Holly Raiche (APRALO) • Carlton Samuels (LACRALO) • Evan Leibovitch (NARALO)	30.09.2013	10.10.2013	14.10.2013	14.10.2013	20.10.2013	21.10.2013	22.10.2013	Mary Wong policy-staff@icann.org	AL-ALAC-ST-1013-01-00-EN

Comment / Reply Periods (*)
Comment Open Date:
24 September 2013
Comment Close Date:
22 October 2013 - 23:59 UTC
Reply Open Date:
23 October 2013
Reply Close Date:
13 November 2013 - 23:59 UTC

Important Information Links
Public Comment Announcement
To Submit Your Comments (Forum)
View Comments Submitted

Brief Overview
Originating Organization:
GNSO
Categories/Tags:

- Policy Processes

Purpose (Brief):
This study, conducted by the National Physical Laboratory (NPL) in the United Kingdom, analyzes gTLD domain names to measure whether the percentage of privacy/proxy use among domains engaged in illegal or harmful Internet activities is significantly greater than among domain names used for lawful Internet activities. Furthermore, this study compares these privacy/proxy percentages to other methods used to obscure identity – notably, Whois phone numbers that are invalid.

These findings will help the community understand the role that privacy and proxy service abuse plays in obscuring the identities of parties engaged in illegal or harmful activities, including phishing, cybersquatting, hosting child abuse sexual images, advanced fee fraud, online sale of counterfeit pharmaceuticals, and more.
Current Status:
This Public Comment solicitation represents an opportunity for the community to consider the study results detailed in this report, provide feedback and request further clarifications. In parallel, ICANN and NPL will conduct Webinars to facilitate feedback by summarizing this study's purpose, methodology, key findings, and conclusions.
Next Steps:
NPL will consider all comments submitted to this Public Comment forum during the comment period, incorporate any needed clarifications, and then publish a final version of this Whois Privacy and Proxy Service Abuse study report. It is expected that this report will inform future GNSO policy development in relation to the Whois system.
Staff Contact:
Mary Wong
Email Staff Contact

Detailed Information
Section I: Description, Explanation, and Purpose:
At the request of the GNSO Council, ICANN engaged the National Physical Laboratory (NPL) in the United Kingdom to test the hypothesis that "*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.*"

To provide empirical data of use to Whois policy-making, NPL set out to measure whether the percentage of privacy/proxy use among domains engaged in various kinds of illegal or harmful Internet activities is greater than among domain names used for lawful Internet activities. Additionally, because privacy /proxy policy changes could prompt malicious registrants to elude contact in other ways, NPL also measured other methods used to obscure perpetrator identity – notably, invalid Whois phone numbers.

This study, led by Dr. Richard Clayton of the University of Cambridge, gathered large representative samples of domain names implicated in various illegal or harmful online activities, ranging from unsolicited phishing, typosquatting, and malware distribution to hosting child abuse sexual images, advanced fee fraud (also known as "419 scams"), and online sale of counterfeit pharmaceuticals. Key technical inputs were also provided by Professor Tyler Moore of Southern Methodist University and Dr Nicolas Christin of Carnegie Mellon University.

By examining sampled incidents and Whois data associated with domain names across the top five gTLDs – .biz, .com, .info, .net and .org – this study measured how often privacy or proxy services were abused by perpetrators (alleged and confirmed). Additionally, these results were compared to privacy /proxy use among domains engaged in lawful and harmless activities (e.g., banks and legal pharmacies), chosen to mirror studied illegal/harmful activities. Finally, researchers attempted to call registrants for a subset of these domain names not using privacy or proxy services, to determine whether they could in fact be contacted with only Whois data.

This draft report summarizes project activities, methodology, sampled data and findings, including statistical analysis of differences observed by the research team. These study findings will help the community understand the role that privacy and proxy service abuse plays in obscuring the identities of parties engaged in illegal or harmful Internet activities.

The GNSO Council is now seeking community review and feedback on the draft report. The purpose of this Public Comment period is to ensure that study results have been communicated clearly and to solicit feedback on desired clarifications (if any).
Section II: Background:
As part of its effort to develop a comprehensive understanding of the gTLD Whois system, the GNSO Council expressed an interest in conducting an in-depth study of privacy and proxy service abuse among gTLD domain names registrants engaged in illegal or harmful Internet activities. At the GNSO's request, ICANN issued a Request for Proposal (RFP) in May 2010 describing a study to methodically analyze a representative sample ofgTLD domains associated with a variety of illegal or harmful Internet activities. By comparing how often these "bad actors" use privacy/proxy services with overall privacy /proxy use, the GNSO hoped to prove or disprove its hypothesis that a significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services in order to obscure the perpetrator's identity.

After considering RFP responses received from researchers willing to undertake this Privacy/Proxy Abuse study, as well as questions raised by both researchers and reviewers, the GNSO Council decided to fund a somewhat revised study proposed by NPL. Specifically, NPL proposed studying many but not all of the illegal/harmful activities enumerated by the RFP, using samples obtained largely from "live feeds" and authoritative sources. NPL declined to study DoS attacks, DNS poisoning, IP theft, and on-line stalking using incidents submitted by victims, questioning their relevance and/or the ability to gather reliably representative samples.

In April 2011, this revised study was approved by the GNSO Council and awarded to NPL. When initiating this study, the GNSO Council asked that the study report expressly note that this study's purpose is only to analyze "bad actors". Notwithstanding the legal or harmless domain names studied here for comparison purposes, many legitimate privacy/proxy customers are unaccounted for within the scope of this study. This study does notattempt to measure privacy/proxy use or Whois accuracy across all gTLDs, as did broader studies such as that performed by NORC at the University of Chicago in 2010.

The findings from this study are intended to provide empirical data needed to understand the role that privacy and proxy service abuse plays in obscuring the identities of parties engaged in illegal or harmful activities. This empirical data will create a baseline for evaluating potential Whois and Privacy/Proxy service policy changes.
Section III: Document and Resource Links:
Whois Privacy and Proxy Service Abuse Study Draft Report [PDF, 624 KB]
Section IV: Additional Information:
Whois Privacy/Proxy Abuse Study Terms of Reference [PDF, 321 KB]

Whois Privacy/Proxy Abuse Study Staff Report [PDF, 437 KB]

GNSO Council Motion April 2011

NPL Selected to Conduct a gTLD Whois Privacy and Proxy Abuse Study

Additional Whois studies have also been conducted at the request of the GNSO Council, as summarized at:http://gnso.icann.org/issues/whois/

(*) Comments submitted after the posted Close Date/Time are not guaranteed to be considered in any final summary, analysis, reporting, or decision-making that takes place once this period lapses.

FINAL VERSION TO BE SUBMITTED IF RATIFIED

Please click here to download a copy of the PDF below.

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The National Physical Laboratory *Study of Whois Privacy and Proxy Service Abuse* tested the following two hypotheses:

- 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; and
- The percentage of domain names used to conduct illegal or harmful Internet activities that are registered via privacy or proxy services is significantly greater than the percentage of domain names used for lawful Internet activities that employ privacy or proxy services.

It found the first hypothesis to be true, and the second, to be partly true. In other words, while the Study acknowledges the many legitimate uses of privacy and proxy services, it points to the use of such services to hide the identify of the perpetrator engaged in the misuse of malicious use of the Internet.

In its final report, the Whois Policy Review Team recommended that ICANN should regulate and oversee privacy and proxy service providers, possibly through an accreditation scheme, that would strike an appropriate balance between privacy, data protection and law enforcement. As part of developing such an accreditation scheme, registrations under the scheme should include full contact details for the domain name user that are 'contactable and responsive.'

The 2013 changes to the RAA included a framework for an accreditation scheme for privacy and proxy services. However, the important elements of such a scheme, particularly the balance between the legitimate needs for privacy, data security and law enforcement, are still to be developed.

The ALAC generally welcomed the many changes to the RAA passed by the Board in 2013. However, the ALAC made two recommendations, the importance of which are underlined by this study.

We supported the development of an accreditation scheme for privacy and proxy services and argued they should only be accredited to the extent they meet all relevant RAA requirements (including accuracy and verification of Whois information for the beneficial user of the domain name). We also said that the new requirements for verification of Whois information should apply not only to registrars (and resellers) but to proxy and privacy service providers as well.

The ALAC supports this study and the clear support it provides for the development of a strong privacy and proxy service provider accreditation scheme and for accuracy and verification requirements covering all Whois information, including those who use privacy and proxy service providers.

FIRST DRAFT SUBMITTED

The National Physical Laboratory *Study of Whois Privacy and Proxy Service Abuse* tested the following two hypotheses:

- 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; and
- The percentage of domain names used to conduct illegal or harmful Internet activities that are registered via privacy or proxy services is significantly greater than the percentage of domain names used for lawful Internet activities that employ privacy or proxy services.

It found the first hypothesis to be true, and the second, to be partly true. In other words, while the Study acknowledges the many legitimate uses of privacy and proxy services, it points to the use of such services to hide the identify of the perpetrator engaged in the misuse of malicious use of the Internet.

In its final report, the Whois Policy Review Team recommended that ICANN should regulate and oversee privacy and proxy service providers, possibly through an accreditation scheme, that would strike an appropriate balance between privacy, data protection and law enforcement. As part of developing such an accreditation scheme, registrations under the scheme should include full contact details for the domain name user that are 'contactable and responsive'

The 2013 changes to the RAA included a framework for an accreditation scheme for privacy and proxy services. However, the important elements of such a scheme, particularly the balance between the legitimate needs for privacy, data security and law enforcement, are still to be developed.

The ALAC generally welcomed the many changes to the RAA passed by the Board in 2013. (link to ALAC statement on the RAA changes of 4 June 2013. However, we made two recommendations, the importance of which are underlined by this study.

We supported the development of an accreditation scheme for privacy and proxy services and argued they should only be accredited to the extent they meet all relevant RAA requirements (including accuracy and verification of Whois information for the beneficial user of the domain name). We also said that the new requirements for verification of Whois information should apply not only to registrars (and resellers) but to proxy and privacy service providers as well.

The ALAC supports this study and the clear support it provides for the development of a strong privacy and proxy service provider accreditation scheme and for accuracy and verification requirements covering all Whois information, including those who use privacy and proxy service providers.