

Community recommendations for Whois privacy/proxy accreditation program

17 October 2012

Below is a summary of public input received by ICANN to date on potential topics for inclusion in a privacy/proxy service accreditation program. These suggestions and considerations were provided by the Whois Review Team (beginning on page 8, below), the GNSO/ALAC Registrar Accreditation Agreement Drafting Team (beginning on page 21), and representatives of the law enforcement community (see <http://www.icann.org/en/resources/registrars/raa/raa-law-enforcement-recommendations-01mar12-en.pdf>.)

| ELEMENTS OF A PRIVACY-PROXY ACCREDITATION PROGRAM | | | |
|--|---|--|---------------------------|
| | Feature | Explanation | Source¹ |
| 1 | Practices & Procedures | | |
| 1.1 | Documentation of Service Practices | These should be clearly published, and pro-actively advised to potential users of these services so they can make informed choices based on their individual circumstances | WHOIS RT |
| 1.2 | Escrow of Customer Data | Require the escrow of privacy or proxy registration data of customer, licensee, or beneficial owner | GNSO-ALAC RAA DT |
| 1.3 | Standardized Relay and Reveal Procedures | Adopting agreed standardized relay and reveal processes and timeframes | WHOIS RT |
| 1.4 | Revealing identity for service of cease & desist Letters in a timely manner | Need to enable service of process in a timely manner in order to avoid flight risk (transfer to another provider to evade service) | WHOIS RT |

¹ Excerpts from the source materials and relevant documents are included in [Annex 1](#)

| | | | |
|-----|--|--|------------------|
| 1.5 | Obligation to forward correspondence | Requirement to forward allegations of malicious conduct, cybersquatting, and other illegal activities to privacy or proxy service customers | GNSO-ALAC RAA DT |
| 1.5 | Revealing in instances of illegal malicious conduct | In instances of presentment of evidence of illegal malicious conduct should result in a requirement to reveal the contact information of customers of privacy or proxy services, consistent with procedures designed to respect any applicable protections for privacy and freedom of expression. | GNSO-ALAC RAA DT |
| 1.6 | Publication in WHOIS in instances of illegal conduct | Registrants using privacy/proxy registration services will have authentic WHOIS information immediately published by the Registrar when registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity. | LEA Request |

| | | | |
|-----|--|--|------------------|
| 1.7 | Accepting Liability if Fails to Reveal | A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly (i.e. within five business days) discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm | GNSO-ALAC RAA DT |
|-----|--|--|------------------|

| | | | |
|----------|-------------------------------------|---|------------------|
| 2 | Relationship with Customer | | |
| 2.1 | Due Diligence | Conducting periodic due diligence checks on customer contact information | WHOIS RT |
| 2.2 | Terminating a Customer's access | Cancel registrations of proxy services that do not fulfill their contractual obligations | WHOIS RT |
| 2.3 | Rights of Customers | Providing clear and unambiguous guidance on the rights and responsibilities of registered name holders, and how those should be managed in the privacy/proxy environment | WHOIS RT |
| 2.4 | Maintenance of Customer Information | Require registrars to collect and preserve contact data for beneficial registrant/licensee even when registration is channeled through proxy or privacy service made available in connection with the registration process. | GNSO-ALAC RAA DT |

| | | | |
|----------|---------------------------------------|--|------------------|
| 3 | Disclosure | | |
| 3.1 | WHOIS Labels | Clearly labeling WHOIS entries to indicate that registrations have been made by a privacy or proxy service | WHOIS RT |
| 3.2 | WHOIS Provider Contacts | Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive | WHOIS RT |
| 3.3 | Relationship with Registrar | Registrars should disclose their relationship with any proxy/privacy service provider | WHOIS RT |
| 4 | Abuse Point of Contact | | |
| 4.1 | Maintain Abuse Point of Contact | Maintaining dedicated abuse points of contact for each provider | WHOIS RT |
| 4.2 | Publication of Abuse Point of Contact | Designation and publication of technically competent point of contact on malicious conduct issues, available on 24/7 basis | GNSO-ALAC RAA DT |
| 5 | Law Enforcement | | |
| 5.1 | Access for Law Enforcement | The ability to hide ones identity in the global e-commerce marketplace creates an environment that allows illegal activities to flourish. It is imperative that law enforcement is able to identify the who, what, where of domain name operators immediately in order to effectively investigate. | WHOIS RT |

| | | | |
|------------|---|---|------------------|
| 6 | Privacy Considerations | | |
| 6.1 | Balancing Privacy and Public Access | Consideration of use of domain name-- commercial v. personal | WHOIS RT |
| 6.2 | Restrict Proxy/Privacy Services to only non-commercial purposes | If proxy/privacy registrations are allowed, the proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only. | LEA Request |
| 7 | Enforcement | | |
| 7.1 | Sanctions and Penalties for Noncompliance | | WHOIS RT |
| 7.2 | De-accreditation of Provider | Clear path for deaccreditation for repeat, serial or otherwise serious breaches | WHOIS RT |
| 7.3 | Transition of Providers | Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy/proxy provider | WHOIS RT |
| 7.4 | Registrar to cancel Registrations | Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal | GNSO-ALAC RAA DT |

| | | | |
|------------|--|--|-------------|
| 8 | Due Diligence on Providers | | |
| 8.1 | Due Diligence in Accreditation Process | ICANN to implement accreditation system for Proxy Services using the same stringent checks and assurances as provided to Registrars, to ensure that all proxy services used are traceable and can supply correct details of registrant to relevant authorities | LEA Request |

ANNEX 1

PRIVACY/PROXY ACCREDITATION PROGRAM DEVELOPMENT

DOCUMENTS FOR CONSIDERATION

I. WHOIS RT Final Report

Excerpts relating to Privacy Proxy:

Definitions:

Working definitions of Privacy and Proxy Services:

- Privacy Service a service that provides the Registrant Name and a subset of other information (possibly null set) but consistent across ICANN
- Proxy Service a relationship in which the registrant is acting on behalf of another. The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.

Recommendation 10: Data Access -- Privacy and Proxy Services

Findings

Privacy and proxy services have arisen to fill an ICANN policy vacuum. These services are clearly meeting a market demand, and it is equally clear that these services are complicating the WHOIS landscape.

Privacy and proxy services are used to address noncommercial and commercial interests, which many view as legitimate. For example,

Individuals – who prefer not to have their personal data published on the Internet as part of a WHOIS record;

Organizations – as religious, political or ethnic minority, or sharing controversial moral or sexual information; and

Companies – for upcoming mergers, new product or service names, new movie names, or other product launches.

However, ICANN's current lack of any clear and consistent rules with regards to privacy and proxy services has resulted in unpredictable outcomes for stakeholders. In terms of the Review Team's scope:

- law enforcement shared its concern over the abuse of proxy services by criminals seeking to hide, companies defrauding customers, and parties attacking the security of the Internet including by botnets and malware; and
- the current use of privacy and proxy services raises questions about whether ICANN is meeting its AoC commitments relating to ‘timely, unrestricted and public access’ to WHOIS data.

The Review Team considers that with appropriate regulation and oversight, privacy and proxy services appear capable of addressing stakeholder needs.

Recommendation 10 - Data Access -- Privacy and Proxy Services

The Review Team recommends that ICANN should initiate processes to regulate and oversee privacy and proxy service providers.

ICANN should develop these processes in consultation with all interested stakeholders.

This work should take note of the studies of existing practices used by proxy/privacy service providers now taking place within the GNSO.

The Review Team considers that one possible approach to achieving this would be to establish, through the appropriate means, an accreditation system for all proxy/privacy service providers. As part of this process, ICANN should consider the merits (if any) of establishing or maintaining a distinction between privacy and proxy services.

The goal of this process should be to provide clear, consistent and enforceable requirements for the operation of these services consistent with national laws, and to strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, data protection, law enforcement, the industry around law enforcement and the human rights community.

ICANN could, for example, use a mix of incentives and graduated sanctions to encourage proxy/privacy service providers to become accredited, and to ensure that registrars do not knowingly accept registrations from unaccredited providers.

ICANN could develop a graduated and enforceable series of penalties for proxy/privacy service providers who violate the requirements, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches.

In considering the process to regulate and oversee privacy/proxy service providers, consideration should be given to the following objectives:

- Clearly labeling WHOIS entries to indicate that registrations have been made by a privacy or proxy service;
- Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive;
- Adopting agreed standardized relay and reveal processes and timeframes; (these should be clearly published, and pro-actively advised to potential users of these services so they can make informed choices based on their individual circumstances);
- Registrars should disclose their relationship with any proxy/privacy service provider;
- Maintaining dedicated abuse points of contact for each provider;
- Conducting periodic due diligence checks on customer contact information;
- Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy/proxy provider.
- Providing clear and unambiguous guidance on the rights and responsibilities of registered name holders, and how those should be managed in the privacy/proxy environment.

From the WHOIS RT Final Report- PART II – ICANN WHOIS Policy and its Implementation:

Chapter 3: The Complex History of WHOIS Policy

D. PROXY and PRIVACY Registrations

A special set of cases exists in which the Registrant seeks additional protections for its personal data so that it will *not* be easily found in globally-available WHOIS databases. The Review Team heard from all members of the ICANN gTLD communities with regard to this type of service.

Specifically, companies, organizations and individuals shared their need, use and value of proxy and privacy services, including:

- For companies where an upcoming merger, new product or service name, new movie name, or other new product launch, involves a domain name which should not yet be directly associated with the business (to avoid market speculation and other negative business consequences). Companies use proxy services or individuals such as attorneys who act as proxies.
- Organizations noted the danger of operating in a country or region in which they are a religious, political or ethnic minority, or share information about moral or sexual issues that may be controversial in some areas, such as gay rights.

- Some private individuals prefer not to have their personal data published on the Internet as part of a WHOIS record.
- Webmasters and Webhosts regularly register domain names for an array of clients as a first step in beginning the development of their websites.

Two types of services have emerged as a market response to the need for special services. Called proxy and privacy services, the terms are used interchangeably, but the Review Team found their meanings have some key differences:

- **Privacy Service** a service that provides the Registrant Name and a subset of other information (possibly null set) but consistent across ICANN.

Proxy Service a relationship in which the registrant is acting on behalf of another. The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.

Law enforcement shared its concern over the abuse of proxy services by criminals seeking to hide, companies defrauding customers, and parties attacking the security of the Internet including by botnets and malware.

The Registrar Accreditation Agreements speak specifically to the issue of registering a domain name through a third party, but do not use the terms “proxy and privacy.” Rather they talk about the “Registered Name Holder” (i.e. the proxy) and the Licensee (i.e. the underlying party on whose behalf the domain name is registered) and require “timely resolution” of problems that may arise:

Ownership and Responsibility of the Domain Name by the Proxy

Section 3.7.7.3, Part 1

2001 and 2009 RAA

Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.

The RAAs also call on Registered Name Holder to be responsible for the “wrongful use” of the domain name unless it “promptly discloses” the current contact information of the licensee on “reasonable evidence of actionable harm.”

Disclosure of the Underlying Licensee

Section 3.7.7.3, Part 2

2001 and 2009 RAA

A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm.

Proxy and privacy services are among the least developed of the WHOIS policy areas. As discussed in Chapter 6, the Review Team heard many complaints about these services from Law Enforcement and others, suggesting that additional policies may be appropriate in this area.

PART III: The Extent to which ICANN’s Existing WHOIS Policy and its Implementation Are Effective in Meeting Stakeholder Needs

Chapter 6: Understanding the Needs of Stakeholders

...

C. Privacy and Proxy Services

The most widespread way of addressing the privacy concerns of some stakeholders is the use of ‘privacy’ and ‘proxy’ services. These services are currently offered commercially by a wide range of service providers, including some registrars, and serve to limit publicly accessible information about domain registrants.

As noted earlier in this report, privacy and proxy services are referred to in provisions 3.4.1 and 3.7.7.3 of ICANN’s RAA, however the terms are currently not well defined or understood. There appears to be some confusion in the community about how they should be used and the differences between them. The Review Team understands that the terms are commonly understood to mean:

- **Privacy Service**-- a service that provides the Registrant Name and a subset of other information (possibly null set) but consistent across ICANN.
- **Proxy Service** -- a relationship in which the registrant is acting on behalf of another. The WHOIS data is that of the agent and the agent alone obtains all rights and assumes all responsibility for the domain name and its manner of use.

The Review Team notes that the use of these services is widespread, with a 2010 study² determining that privacy and proxy services are used in 15%-25% of WHOIS records.

There are diverging views from stakeholders about the use of privacy and proxy services. For example, the Noncommercial Users Constituency argued that:

ICANN should recognize that privacy and proxy services fill a market need; the use of these services indicates that privacy is a real interest of many domain registrants.³

On the other hand, one law enforcement agency argued that ‘if an entity is engaged in legitimate business activities, then a proxy service should not be necessary’. Another stated that ‘privacy/proxy services can be abused’, and that ‘criminals do use proxy and privacy registrations to hide their identities’.

Do Privacy and Proxy Services Undermine WHOIS?

A significant number of public responses to the WHOIS discussion paper, and input from law enforcement agencies via the review team’s targeted questionnaire, argued that privacy and proxy services undermine the effectiveness of the WHOIS service, both in terms of its ability to meet the legitimate needs of law enforcement and to promote consumer trust. One law enforcement agency argued that:

proxy services play right into the hands of organized crime, they hide all their business behind them and this is a huge issue, not only for law enforcement, but for the wider internet community as a whole.

Another law enforcement agency argued that:

“The time routinely invested by law enforcement to validate WHOIS data that may be false, unavailable, incomplete, or proxied impedes investigations”.

Similarly, the InterContinental Hotels Group argued that:

privacy services have frequently frustrated our ability to protect our hotel brands online, which, unfortunately, often leads to confusion and other problems among consumers.⁴

Some respondents to the Discussion Paper also questioned whether the use of privacy and proxy services was consistent with ICANN’s commitment to the provision of unrestricted public access to complete WHOIS data. For example, Time Warner urged the review team to:

² <http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf>

³ Non-Commercial Users Constituency, NCUC, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00014.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

⁴ InterContinental Hotels Group, IHG, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00010.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

identify the proliferation of proxy registration services, and the consequent inaccessibility and inaccuracy (for all practical purposes) of a huge swath of gTLD WHOIS data, as a major flaw in ICANN's implementation of its WHOIS policies.⁵

The Coalition for Online Accountability also stated that:

Until ICANN is able to bring some semblance of order, predictability and accountability to the current 'Wild West' scenario of proxy registrations, it will be impossible to make significant progress toward improving the accuracy of WHOIS data, so that the service can better fulfill its critical function to internet users and society as a whole.⁶

Other stakeholders argued that some way protect registrant information is needed. For example, the Noncommercial Users Constituency wrote:

Privacy and accuracy go hand-in-hand. Rather than putting sensitive information into public records, some registrants use "inaccurate" data as a means of protecting their privacy. If registrants have other channels to keep this information private, they may be more willing to share accurate data with their registrar.⁷

Other groups argued in oral comments that proxy/privacy services, as private entities, are outside the scope of ICANN to regulate, and in many cases, are not apparent to the registrars (as in a lawyer registering domain names for a client).

In a discussion of the WHOIS Review Team and the Intellectual Property Constituency, the use of proxy and privacy services arose and the beneficial use of the services to protect trade secret and confidential commercial information was noted (e.g., as in the name of an upcoming movie, a new product or service, or a potential acquisition target together with the proposed new name of the entity).

Thus, in spite the broad level of concern about privacy and proxy services, a significant number of concerned respondents to the public Discussion Paper and law enforcement questionnaire viewed them as serving legitimate needs and did not advocate for their abolition. For example, some law enforcement agencies noted that privacy and proxy services are a 'tool to remain anonymous which may be useful and justified in certain limited cases', such as 'if someone has a Family Protection Order (or similar) and displaying their information may put them at risk of harm'.

⁵ Time Warner Inc., comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00013.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

⁶ Coalition for Online Accountability, COA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00020.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

⁷ Non-Commercial Users Constituency, NCUC, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00014.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

Rather than arguing against the use of proxy and privacy services *per se*, many stakeholders identified the unregulated environment in which they operate as a major underlying problem. For example, Time Warner noted that while it did ‘not oppose the concept of proxy registration in limited circumstances’, it did see:

the development of a vast universe of 20 million or more gTLD domain name registrations, for which the identity and contact data of the registrant is hidden and, all too often, completely inaccessible, [as] a direct attack on ICANN’s chief policy goal for WHOIS.⁸

Similarly, the Coalition for Online Accountability (COA) acknowledged that some registrants may require specific privacy protection, but these only accounted for ‘an infinitesimal fraction’ of current privacy and proxy registrations, and that the:

creation of a vast unmanaged database of tens of millions of effectively anonymous domain names ... is an irrational and socially damaging ‘solution’, one that inflicts far greater costs than warranted upon legitimate e-commerce, consumer interests, law enforcement and the public at large.⁹

But the At-Large Advisory Committee (ALAC) suggests that valuable interests on both sides can be balanced:

The Team may be able to acknowledge the instance of Privacy Proxy Services and the role they play in the WHOIS ecosystem and chart and recommend some workable solution that acknowledges and fully embraces privacy concerns of the community, including ways that these may be answered in a balanced way.¹⁰

Specific concerns with the current unregulated environment include that:

- it impedes investigations and makes determination of the competent jurisdiction difficult. In this context, one law enforcement agency argued that they are ‘aware of an online company providing a domain privacy protection service that actively promotes that they are uncontactable by any other means except through their website. This service is regularly utilized by criminals to register criminal based domains;
- it increases risk for law enforcement agencies by exposing investigative activities to unknown and untrusted parties. The Business Constituency clearly illustrates this risk when

⁸ Time Warner Inc., comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00013.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

⁹ Coalition for Online Accountability, COA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00020.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

¹⁰ At-Large Advisory Committee, ALAC, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00020.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00026.html>

it states that its members have ‘experienced situations where the registrar’s ‘proxy service’ is simply a shell behind which to shield the registrar’s own cybersquatting and illegal activities’; and

- the responsiveness of proxy or privacy service providers varies widely, with no current recourse for failure to disclose data.

In terms of responsiveness, the Motion Picture Association of America (MPAA) stated that:

To date, only one proxy service has complied with MPAA requests to reveal contact information that would enable the service of a cease and desist notice to suspect operators. Seven other have refused to do so or have simply not responded. Even the one more compliant service has recently changed its policies so that it takes up to ten days or more (after notifying its customer) before it will disclose the information. This gives the suspect ample time to transfer the domain name to another suspect entity or take other steps to evade detection.¹¹

Similarly, Time Warner argued that:

Whether or not a member of the public would ever be able to learn the identity or be able to contact the party actually responsible for the registration ... depends entirely on whether this proxy registration provider chooses to make that information available. In Time Warner’s experience, some proxy registration providers are responsible, and will divulge this information upon being presented with evidence that the registration is being used to carry out abusive activities. Many others, however, do not.¹²

Balancing Privacy and Public Access

To address these concerns about lack of regulation of privacy and proxy services, several respondents to the public Discussion Paper and the law enforcement questionnaire argued that:

ICANN needs to regulate privacy service providers.

In most cases, respondents argued that:

this should include the accreditation of service providers and the imposition of minimum conditions for their operation.

For example, the Intellectual Property Constituency argued that:

¹¹ Motion Picture Association of American, MPAA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00020.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00016.html>

¹² Time Warner Inc., comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00013.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

ICANN should undertake to create an official set of guidelines for what constitutes a valid privacy/proxy service and best practices for such services.¹³

Several law enforcement agencies suggested that:

this type of regulation could mitigate some of their concerns with privacy services, and assist in the investigation and shut down of criminal domains.

Suggestions for regulatory conditions put forward by respondents to the public Discussion Paper and the law enforcement questionnaire related to the development of clear, workable, enforceable, and standardized processes to regulate access to registrant data when requested. For example, the International Trademark Association recommended that:

where a domain has been registered using a privacy or proxy service, there should be clear, enforceable contract mechanisms and procedures for the relay of communications to the beneficial owner, and for revealing the identity and contact information of the beneficial owner ... privacy/proxy services should be governed by a uniform body of rules and procedures that is overseen by ICANN, including standardized relay and reveal processes.¹⁴

Several stakeholders also emphasized the need to limit their use of privacy services in various ways – for example, to private individuals not involved with selling products or otherwise collecting or soliciting money.

Another issue raised by respondents to the public Discussion Paper and the law enforcement questionnaire relates to which data fields should be able to be limited by a privacy service. This issue is central to reaching an appropriate balance between personal privacy and ICANN’s commitment to publicly available information. In this context, one law enforcement agency argued that:

it is really important to keep in mind the right of the Internet users to receive reliable data about the owners and registrants of the domain names providing services for them. Privacy protection should not infringe upon the right to receive accurate and complete WHOIS data.

As noted above, several respondents argued that there may be a case to limit access to some registrant information, and some respondents focused on specific data fields (such as personal addresses, phone numbers and email addresses). For example, Nominet stated that within the .uk ccTLD:

¹³ Intellectual Property Constituency, IPC, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00019.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

¹⁴ International Trademark Association, INTA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00011.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

In line with UK data protection law, a registrant who is a non-trading individual can opt to have their address omitted from the WHOIS service.¹⁵

Similarly, another commenter argued that:

Balancing privacy, security and the right to know is the question. Minimal data requirements that allow a quick identification would be ideal, like Registered Name Holder, State/City/Country, email and telephone.¹⁶

In terms of balance, some respondents argued that it was important to retain enough publicly available data to establish domain name ownership and registrant identity. For example, the International Trademark Association argued that:

INTA supports open access to ownership information for every domain name in every top-level domain ... Available information should include the identity of and accurate, reliable contact details for the true owner of the domain name.¹⁷

The question of ownership and identity is central to the distinction between privacy and anonymity, and several stakeholders raised specific concerns about lack of public access to a registrant's name and identity. For example, one law enforcement agency argued that:

The ability to hide ones identity in the global e-commerce marketplace creates an environment that allows illegal activities to flourish. It is imperative that law enforcement is able to identify the who, what, where of domain name operators immediately in order to effectively investigate.

While several law enforcement agencies argued that privacy services could be regulated to provide special access to underlying registrant data (including registrant name) for law enforcement agencies, this would not address the broader consumer trust concerns associated with anonymity. For example, International Trademark Association (INTA) argues that:

In most circumstances, publishing on the internet is a public act, and the public should be able to determine who they are dealing with.¹⁸

¹⁵ The Review Team notes that this is consistent with ICANN-approved arrangements in place in the UK based Telnic. Nominet, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00018.html> the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

¹⁶ Fatima Cambronero, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00023.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

¹⁷ International Trademark Association, INTA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00011.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

¹⁸ International Trademark Association, INTA, comments <http://forum.icann.org/lists/whoisrt-discussion-paper/msg00011.html> on the WHOIS Policy Review Team Discussion Paper, <http://forum.icann.org/lists/whoisrt-discussion-paper/>

The GAC WHOIS Principles similarly note that WHOIS data can contribute:

to user confidence in the Internet ... by helping users identify persons or entities responsible for content and services online.¹⁹

The clear feedback from a range of stakeholders was that they found it important that WHOIS data should be accurate. There were a number of suggestions about what factors may be contributing to the current high levels of data inaccuracy.

On availability, two conflicting, but legitimate expectations were expressed by stakeholders: first, that the data should be freely available; and secondly, there was a recognition that total availability causes conflicts with legitimate expectations of privacy.

Numerous comments were made about the industry of commercial proxy and privacy providers which has grown up over the past decade.

In its Singapore Communiqué, the GAC emphasized “the need for effective compliance activities, noting that legitimate users of WHOIS data are negatively affected by non-compliance.”

WHOIS RT Final Report

Chapter 7: Gap Analysis

E. The Proxy Registration System

Review Team members are in unanimous agreement that the status quo regarding proxy registrations is not sustainable, is not fair to legitimate participants in the domain name marketplace, frustrates valuable social goals such as law enforcement and the protection of intellectual property, and reflects poorly on ICANN's commitment to serve the public interest.

We are also in agreement that the goal should be to give accredited registrars strong incentives not to foster this undesirable status quo, and that such incentives should arise both from the terms of the ICANN contracts with registrars, and from principles of legal responsibility under national law. ICANN can control the first source of these incentives; its contractual provisions may influence, but cannot control the second, since neither of the parties most directly involved - the proxy service customers, and the law enforcement or other party seeking to identify them and hold them accountable - is under contract to ICANN.

We have reached consensus on all the recommendations set out below. We request that the next WHOIS Review Team reviews the privacy and proxy industry's progress in this regard, and in the event

¹⁹ https://gacweb.icann.org/download/attachments/1540132/WHOIS_principles.pdf?version=1&modificationDate=1312460331000

that it finds the WHOIS policy and its implementation unsatisfactory at that point, we trust that it will make recommendations for more concrete measures.

Ultimately, ICANN's WHOIS policy and implementation in the area of proxy and privacy services cannot be effective or successful without proactive ICANN compliance measures, e.g. to press registrars to cancel registrations of proxy services that do not fulfill their contractual obligations as set forth in the RAA. A well-resourced and credible compliance program is essential to reforming the unacceptable status quo in this area.

II RAA-DT Final Report

From the 12 High Priority Items:

| Item No. | Description | Cross-reference (RAA matrix) | Comments |
|----------|--|--------------------------------------|--|
| 3 | Designation and publication of technically competent point of contact on malicious conduct issues, available on 24/7 basis | 3.4; 3.5; 5.4 | Requirement for registrars; possible requirement for resellers and proxy-privacy services |
| 4 | Registrar disclosure of privacy/proxy services made available in connection with registration; and responsibility of registrar for compliance by such services | 5.2 | Could also apply to such service made available by resellers. Includes, but not limited to, alter ego services |
| 5 | Obligations of privacy/proxy services made available in connection with registration re data escrow; Relay function; Reveal function | 5.1; 5.3; 5.5; 5.6; 5.7; 5.10 | See following item for privacy/proxy services not made available in connection with registration |
| 6 | Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal | 5.8; 5.10 | This applies to proxy services not offered by the registrar in connection with registration, i.e., independent services. This is where Relay or Reveal function requirements for these services could be spelled out |

EXCERPTS FROM RAA MATRIX FROM THE RAA-DT FINAL REPORT

| 5 | Privacy/Proxy Services | | | | | |
|-----|---|-------|--------|--|--|--|
| 5.1 | Privacy/Proxy Services- Escrow Requirements and additional disclosure obligations and Resellers | 3.4.1 | Staff | Insert provisions in the RAA that require a registrar and its resellers to escrow privacy or proxy registration data, and at a minimum, disclose the points of contact for privacy or proxy service providers and a description of the privacy or proxy services offered to their customers. | Develop and implement the program in RAA Section 3.12.4 of the RAA giving ICANN the ability to establish or “make available a program granting recognition to resellers that escrow privacy or proxy registration data”. Create a similar contractual provision in RAA Section 3.4.1 for registrars. | Escrow/data collection and preservation; Priority: High |
| 5.1 | | | IPC WG | Explicit requirement for all proxy and private registration services to escrow contact data on beneficial registrant/licensee. | | Priority: High |

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|---|-------------|-------------------|--|--|--|
| 5.1 | | 3.4.1 | Danny Younger | <p>Conspicuous Notice-</p> <p>“display a conspicuous notice to such customers at the time an election is made to utilize such privacy or proxy service that their data is not being escrowed.” --</p> <p>eliminate this clause</p> | | Priority: High |
| 5.2 | <p>Registrars to list privacy/proxy services offered and description of services</p> | 3.4.1 | Staff | | <p>Require registrars on an annual basis to provide a list of privacy or proxy registration services, including points of contact for privacy or proxy service providers and a description of the services provided or made available by a registrar to its customers. This information could be provided either directly to ICANN or published by a registrar on its web site. This requirement would assist ICANN in determining compliance with RAA Section 3.4.1 related</p> | Priority: High (disclosure obligation) |

| | | | | | | |
|--|--|--|--|--|---------------------------------|--|
| | | | | | to escrow of Whois information. | |
|--|--|--|--|--|---------------------------------|--|

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|---|-------------|-------------------|--|--|------------------------------------|
| 5.3 | Proxy/Privacy Services to forward correspondence | | Staff | (2) Insert in RAA Section 3.7.7.3 provisions that require privacy or proxy services to forward allegations of malicious conduct, cybersquatting, and other illegal activities to privacy or proxy service customers. | (1) Require privacy/proxy registration services to forward correspondence to its customer related to specific disputes or alleged disputes involving the domain name. | RELAY function – Priority: High |
| 5.4 | Proxy/Privacy Services to provide Point of Contact for malicious conduct | | Staff | | (2) Require privacy/proxy registration services to provide to ICANN, upon its request, “point of contact” for any privacy or proxy registration services offered or made available to registrar's customers that are responsible for investigating and responding to malicious conduct complaints. | Priority: High (see 5.2) |

| | | | | | | |
|-----|---|---------|-------|--|---|----------------------------------|
| 5.5 | Clarify "Reasonable Evidence of Actionable Harm" Language | 3.7.7.3 | Staff | | (3) Develop contract language and/or advisories that clarify the language of RAA Section 3.7.7.3, including the definition of "reasonable evidence of actionable harm" with input from registrars and non-contracted parties. | REVEAL function – Priority: High |
|-----|---|---------|-------|--|---|----------------------------------|

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|---------------------------------------|-------------|-------------------|--|---|----------------------------------|
| 5.6 | Proxy/Privacy Services to reveal data | | Staff | | (4) The GNSO could discuss what forms of illegal malicious conduct and what standard of evidence should result in a requirement to reveal the contact information of customers of privacy or proxy services, consistent with procedures designed to respect any applicable protections for privacy and freedom of expression. | REVEAL function – Priority: High |
| 5.6 | | | IPC WG | Specify circumstances under which proxy registration services are required to disclose actual contact data of beneficial registrants and licensees, and apply the same standards to private registration services. | | Priority: High |

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|---|-------------|---------------------------------|--|------------------------|-----------------------------|
| 5.6 | | | Law Enforcement Agencies | Registrants using privacy/proxy registration services will have authentic WHOIS information immediately published by the Registrar when registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity. | | Priority: High |
| 5.7 | Registrars to collect customer data for Proxy/Privacy Services | | IPC WG | Require registrars to collect and preserve contact data for beneficial registrant/licensee even when registration is channelled through proxy or privacy service made available in connection with the registration process. | | Priority: High (see 5.1) |

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|--|-------------|-------------------|--|------------------------|---------------|
| 5.8 | ICANN to accredit proxy/privacy services | | IPC WG | ICANN to accredit all proxy or privacy registration services, and registrars prohibited from accepting registrations from unaccredited services. | | Priority: Low |

| | | | | | | |
|-----|--|--|--------------------------|---|--|--|
| 5.8 | | | Law Enforcement Agencies | <p>If proxy/privacy registrations are allowed, registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services. ICANN to implement accreditation system for Proxy Services using the same stringent checks and assurances as provided in these points, to ensure that all proxy services used are traceable and can supply correct details of registrant to relevant authorities.</p> | | <p>LE: Need to explore how the registrar would be able to identify whether a third party proxy service has been used by registrants. Need to also consider how the registrar would be able to access the underlying information for registrants for proxy/privacy services that are offered by third parties.</p> <p>Priority: Low</p> |
|-----|--|--|--------------------------|---|--|--|

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|-----|--|-------------|-------------------|---|------------------------|----------------|
| 5.8 | Registrars responsible for proxy/privacy service compliance with RAA obligations | | IPC WG | Make registrars responsible for compliance with all RAA obligations by providers of proxy or private registration services that are made available in connection with the registrar's registration process. | | Priority: High |

| | | | | | | |
|-----|--|--|---------------------------------|---|--|---------------|
| 5.9 | RAA should not condone or encourage Proxy/Privacy Services | | Law Enforcement Agencies | <p>The RAA should not explicitly condone or encourage the use of Proxy Registrations or Privacy Services, as it appears in paragraphs 3.4.1 and 3.12.4. This goes directly against the Joint Project Agreement (JPA) ICANN signed with the United States Department of Commerce on September 25, 2006 which specifically states "ICANN shall continue to enforce existing (Whois) policy", i.e., totally open and public WHOIS, and the September 30, 2009, Affirmation of Commitments, paragraph 9.3.1 which states "ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing,</p> | | Priority: Low |
|-----|--|--|---------------------------------|---|--|---------------|

| | | | | and administrative contact information.” Lastly, proxy and privacy registrations contravene the 2007 GAC Principles on WHOIS. | | |
|------|--|-------------|-------------------|---|---|----------------------------------|
| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
| 5.10 | Required time to disclose identity of Licensee | 3.7.7.3 | Staff | Incorporate in RAA Section 3.7.7.3 a provision that clarifies the period of time in which a Registered Name Holder must disclose the current identity and contact information of a licensee when a Registered Name Holder does not intend to accept liability for harm caused by the wrongful use of a Registered Name. | Amend the language in RAA Section 3.7.7.3 as follows: “A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly (i.e. within five business days) discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm.” | REVEAL function – Priority: High |

| No. | Issue | RAA Section | Stakeholder Input | Stakeholder Recommendation | Implementation Options | Notes |
|------|--|-------------|---------------------------------|--|------------------------|---------------|
| 5.11 | Restrict Proxy/Privacy Services to only non-commercial purposes | | Law Enforcement Agencies | If proxy/privacy registrations are allowed, the proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only. | | Priority: Low |

III Privacy-Proxy Registration Services Study Conducted by Compliance:

<http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf>

And the Summary of Public Comment on this Report:

<http://forum.icann.org/lists/privacy-proxy-study-report/msg00007.html>

IV WHOIS Proxy/Privacy Reveal & Relay Feasibility Survey

<http://gnso.icann.org/bitcache/43d3fdf651136a4f44073e915add1f07e8a65d11?vid=36483&disposition=attachment&op=download>

V NORC DRAFT WHOIS ACCURACY STUDY

<http://www.icann.org/en/resources/compliance/reports/whois-accuracy-study-17jan10-en.pdf>