Report on the Conclusion of the 2013 Registrar Accreditation Agreement Negotiations

STATUS OF THIS DOCUMENT

This Report on the Conclusion of the 2013 Registrar Accreditation Agreement (RAA) Negotiations is issued by ICANN Staff to the GNSO Council to identify the policy issues remaining from the RAA negotiations to be addressed in the GNSO policy development process (PDP) on the RAA requested by the ICANN Board on 28 October 2011.

SUMMARY

This ICANN Staff report is submitted to the GNSO Council upon the conclusion of the 2013 RAA negotiations, as referenced in the Final Issue Report on the RAA dated 6 March 2012, for the purpose of identifying the policy issues remaining from the RAA negotiations to be explored in the PDP initiated by the ICANN Board.

Table of Contents

I. Executive Summary

On 27 June 2013, the ICANN Board approved the new 2013 Registrar Accreditation Agreement ("2013 RAA"). The objective of this Staff Report is to:

(i) Provide a brief summary to the GNSO Council on how the 2013 RAA addresses the recommended amendments previously proposed by the GNSO-ALAC Drafting Team in its Final Report ("RAA Final Report")[1] and Law Enforcement Agencies ("LEA"); and

(ii) Identify which issues remain to be addressed by the GNSO Policy Development Process ("PDP") on the RAA, requested by the ICANN Board on 28 October 2011 at the ICANN meeting in Dakar through Board Resolution 2011.10.18.33[2].

This Report also provides a brief procedural history for the current status of the RAA Remaining Issues PDP and a suggested roadmap for the issues to be covered by the RAA Remaining Issues PDP Working Group ("WG") that will have to be convened.

As described in greater detail below, out of all the LEA and GNSO-ALAC High Priority Recommendations established at the outset of the RAA negotiations, two recommendations have not been adequately addressed by the completed negotiations:

1) Clarification of registrar responsibilities in connection with proceedings under the existing Uniform Dispute Resolution Policy ("UDRP"); and
2) Issues related to privacy and proxy services – including accreditation and Reveal/Relay procedures.

However, since the GNSO has recently addressed[3] the issues pertaining to a registrar's responsibilities in connection with the locking of a domain name subject to UDRP proceedings, it is staff's opinion that this

[1] See http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf.
[2] See http://www.icann.org/en/groups/board/documents/resolutions-28oct11-en.htm#7

issue no longer needs to be addressed through the RAA Remaining Issues PDP. Further, the UDRP is scheduled to be reviewed by the GNSO eighteen months after the launch of the first generic top-level domain ("gTLD") under ICANN's New gTLD Program[4]. As a result, staff has identified the issues related to privacy and proxy services as the only remaining issue upon the conclusion of the RAA negotiations suited for a PDP, as requested by the ICANN Board.

In preparing this Report, Staff reviewed the various community efforts relevant to topics previously identified for the RAA negotiations, including the 2010 RAA Final Report prepared by the joint GNSO/ALAC Drafting Team on RAA Amendments, requests made by the law enforcement community, and the WHOIS Review Team's Final Report from May 2012. Staff compared the recommendations and priorities described in these documents with the outcomes of the RAA Negotiations (including specific provisions and specifications in the 2013 RAA, as approved by the ICANN Board), and prepared an issues chart on privacy and proxy services (see Section VIII) that is intended to assist the GNSO PDP Working Group on these remaining issues under the RAA. The GNSO PDP is expected to inform ICANN's proposed Action Plan to launch an accredited privacy/proxy program and further ICANN's ongoing efforts to implement the recommendations made by the WHOIS Review Team.

Staff therefore recommends that the GNSO Council proceed to commence the RAA Remaining Issues PDP, as has been requested by the ICANN Board, to address the privacy/proxy services accreditation issues as soon as possible. Staff further recommends that in convening the PDP Working Group, the GNSO Council explicitly charter the Working Group to consider how its recommendations may inform the proposed accredited privacy/proxy program, taking into account the recommendations made by the WHOIS Review Team and other GNSO efforts relating to the issue, such as the Privacy & Proxy Abuse study commissioned by the GNSO Council in 2010, which report is expected to be finalized and published for public comment in time for the Working Group to consider its findings.

---

[3] For additional information, please refer to the GNSO Council's Resolution adopting the recommendations of the Working Group for the PDP on the Locking of a Domain Name subject to UDRP Proceedings: http://gnso.icann.org/en/council/resolutions#201308

[4] See the GNSO Council's Resolution requesting the delivery of an Issue Report on the UDRP and other rights protection mechanisms in both existing and new gTLDs no later than eighteen months after the launch of the first new gTLD: http://gnso.icann.org/en/council/resolutions#201112

II. Background

At the ICANN Meeting in Dakar in October 2011 the ICANN Board adopted Resolution 2011.10.18.32 regarding amendments to the Registrar Accreditation Agreement (the "Dakar RAA Resolution").

The Dakar RAA Resolution directed negotiations on amending the 2009 RAA to be commenced immediately, so as to result in proposed amendments to be published for consideration at the ICANN Meeting in Costa Rica in March 2012. The Dakar RAA Resolution clarified that the subject matter of the negotiations was to include the recommendations made by LEA, those made in the RAA Final Report, as well as other topics that would advance the twin goals of achieving registrant protection and domain name system ("DNS") stability. This resolution further requested the creation of an Issue Report to undertake a GNSO PDP as quickly as possible to address any remaining items not covered by the negotiations and otherwise suited for a PDP.

In response to the Dakar RAA Resolution, ICANN published the Final GNSO Issue Report on RAA Amendments on 6 March 2012. In this Final Issue Report, ICANN staff recommended that the GNSO Council commence a PDP on the RAA contractual amendments upon either: (i) receipt of a report that the RAA negotiations have concluded, or that any of the 24 Proposed Amendment Topics identified in the Final Issue Report are no longer actively being negotiated, or (ii) a Board instruction to proceed with a PDP on any or all of the Proposed Amendment Topics identified in the Final Issue Report.

On 27 June 2013, the ICANN Board approved the new 2013 Registrar Accreditation Agreement (" 2013 RAA"). Upon delivery of this Report, the GNSO Council may now proceed with the Board-requested PDP on the remaining issues established at the outset of the RAA negotiations that were not addressed in the 2013 RAA.

III. Recommendations from the Final Issue Report on the RAA

At the time that the Preliminary Issue Report on RAA Amendments was published in December 2011, it was unknown how many of the 24 Proposed Amendment Topics would be subject to a PDP and Staff expressed its concern that managing one PDP for all of the Proposed Amendment Topics may be overwhelming for the

community volunteers and the Staff. In the Preliminary Issue Report, Staff suggested that the GNSO Council consider dividing these Proposed Amendment Topics into four separate PDPs.

Staff committed to inform the GNSO Council at the conclusion of the RAA negotiations as to which of the Proposed Amendment Topics remained unaddressed in the negotiated new form of the RAA. Staff further suggested that, upon receiving this information, the GNSO Council could consult with the Board to obtain information on the scope, timing, and priority of the PDP to be initiated on these "remaining items," and whether these items should be addressed in one or more PDPs, as described above.

On 22 April 2013 ICANN posted the proposed final 2013 RAA for public comment. The ICANN Board approved the final version of the 2013 RAA, which incorporates changes to reflect public comments received, on 27 June 2013. The Board's approval of the 2013 RAA also represented the formal conclusion of negotiations.

In line with staff's prior recommendations and stated intentions, ICANN is providing this Report to inform the GNSO Council about the remaining issues from the Proposed Amendment Topics - namely, the issues surrounding Proxy/Privacy Services - which fall within the scope of the RAA Remaining Issues PDP, and to suggest an approach with regard to the issues to be addressed in the PDP.

IV. Priority proposed amendments addressed in the 2013 RAA

During the ICANN Dakar Meeting, ICANN and the Registrar Stakeholder Group ("RrSG") announced their agreement to commence negotiations on possible amendments to the RAA to address recommendations made by LEA and in the RAA Final Report, to provide increased protections for registrants, to enhance security generally, and to increase predictability for all stakeholders.

ICANN and the RrSG agreed to discuss the following topics in the negotiations:

- The LEA RAA recommendations, including those as formulated by the LEA in its proposed code of conduct;
- The "High Priority" recommendations from the RAA Final Report (see Final Report);
- To the extent time permits, the "Medium Priority" recommendations from the RAA Final Report; and

- Other topics that would advance the goals of registrant protection, DNS stability, and increased predictability for all stakeholders.

As demonstrated in the charts that follow below, the 2013 RAA addresses the LEA RAA recommendations and the "High Priority" recommendations of the RAA Final Report, as well as most of the "Medium Priority" recommendations in the RAA Final Report.

The highlights of the 2013 RAA[5] include:

- All 12 LEA Recommendations, which served as the impetus for the negotiations, are addressed in the new RAA. The Law Enforcement Summary Chart provided in Section VII below identifies the section or specification of the 2013 RAA that addressed each recommendation. Some of the highlights include the creation of an abuse point of contact at each registrar, WHOIS verification and validation requirements at the registrant and the account holder levels, stronger language on registrar obligations for resellers, and new data retention obligations.
- Enhanced Compliance Tools including broader suspension and termination tools, clarification of audit rights and access to information to facilitate ongoing investigations, and annual certification requirements.
- A Registrant Benefits and Responsibilities Document that sets out, in clear and simple language, the benefits and responsibilities that are laid out in the 2013 RAA, such as the types of information that registrants can expect to be made available to them about terms and conditions of registrations, fees and customer service processes. The document also emphasizes the registrant's role in providing accurate contact information, and responsibilities in maintaining domain name registrations. These enumerated benefits and responsibilities are not comprehensive of all registrant rights and responsibilities set out in consensus policies; however this document is closely tied to the terms of the 2013 RAA.
- Registrar Responsibility for Reseller Compliance with all appropriate terms of the 2013 RAA.

[5] For more information, see ICANN's RAA Posting Memorandum dated 22 April 2013, posted in the Public Comment Forum for the Proposed Final 2013 RAA.

V. Remaining Issues After Close of RAA Negotiations

As exhibited in the following charts below, out of all the LEA and GNSO-ALAC High Priority Recommendations established at the outset of the RAA negotiations, two remained not adequately addressed by the completed negotiations: 1) Clarification of registrar responsibilities in connection with proceedings under the existing Uniform Dispute Resolution Policy ("UDRP"); and 2) Privacy/Proxy Services – including accreditation and Reveal/Relay procedures.

The UDRP-related recommendation has been addressed in the recommendations that were recently adopted by the GNSO Council for the locking of a domain name subject to UDRP proceedings. These recommendations are expected to be considered shortly by the ICANN Board following the closing of the public comment forum (see http://www.icann.org/en/news/public-comment/locking-domain-name-recommendations-02aug13-en.htm).

With regard to the Privacy/Proxy Services Accreditation recommendation, the 2013 RAA provides an interim specification that will be in place until the earlier of 1 January 2017 or until any PDP recommendations are developed by the GNSO and adopted by the ICANN Board. The specification includes a limited set of minimum requirements which comprise: 1) disclosure of key service terms; 2) publication of infringement/abuse point of contact; 3) publication of business contact information; and 4) escrow of customer data.

ICANN and the Registrars' Negotiating Team agreed to a number of interim protections to be in place for proxy and privacy services offered through registrars or their affiliates. These interim protections require that information is made available on items such as customer service processes and when a provider will relay information on the underlying user of the domain name registration. While these are not comprehensive of the protections that can be put in place for proxy and privacy providers, these interim protections are intended to provide a more responsible marketplace until a formal accreditation program is developed by ICANN.

As a result, the Privacy/Proxy Services-related amendment recommendations are the one issue remaining to be addressed by the RAA Remaining Issues PDP.

VI. Treatment of the Priority Amendments from the GNSO/ALAC RAA-DT Final Report

The following chart summarizes the High Priority Items identified in the RAA Final Report, indicates whether they have been addressed in the 2013 RAA, and, where that is the case, lists the applicable section or specification in the 2013 RAA.

SUMMARY OF GNSO-ALAC HIGH PRIORITY AMENDMENTS IN THE 2013 RAA

Item No.	Description	Section
1 Yes	Prohibition on registrar cybersquatting	RAA 5.5.2.3-5.5.2.4
2 Yes	Malicious conduct – registrar duty to investigate	RAA 3.18
3 Yes	Designation and publication of a technically competent point of contact on malicious conduct issues (24 /7)	RAA 3.18.2
4 Yes	Disclosure of privacy/proxy services made available by registrar; Responsibility of registrar for compliance by such services	Registrar Information Spec; RAA 3.12.4, 3.14 and Privacy/Proxy Spec
5 Yes	Obligations of privacy/proxy services made available by registrar re: Data escrow; Relay function; Reveal function	Privacy/Proxy Spec
6 No	Registrar responsibility for cancellation of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal	Reveal/Relay procedures deferred to GNSO PDP

Item No.		Description	Section
7	Yes	Define circumstances under which registrar is required to cancel registration for false Whois data and set reasonable time limits for registrar action	WHOIS Accuracy Specification
8	Yes	Require PCI compliance or similar pre-existing standard that would assist in verification of registrants in registration process	WHOIS Accuracy Specification
9	Yes	Define "reseller" and clarify registrar responsibility for reseller compliance	RAA Sections 1.1 and 3.12
10	Yes	Require greater disclosure of registrar affiliates/multiple accreditations	Registrar Information Specification
11	Yes	Require greater disclosure of registrar contact information, information on form of business organization, officers, etc.	Registrar Information Specification
12	No	Clarification of registrar responsibilities in connection with UDRP proceedings	GNSO PDP on UDRP to address issue

The following chart summarizes the medium-high Priority Items identified in the RAA Final Report, indicates whether they have been addressed in the 2013 RAA and, where that is the case, lists the applicable section or specification in the 2013 RAA.

SUMMARY OF GNSO/ALAC MEDIUM PRIORITY AMENDMENTS IN THE 2013 RAA[6]

✓	Spell out registrar "verification" process after receiving false Whois data report- *WHOIS Accuracy Specification*
✓	Require links to Whois Data Problem Reporting System - *WHOIS Specification*
✓	Service Level Agreement on Whois availability- WHOIS Specification
✓	Disclosure of resellers– *Additional Registrar Information; RAA 3.12.3*
✓	Expand scope of authority to terminate accreditation- *RAA 5.5.2*
✖	Require registrars to report data breaches
✓	Streamline arbitration process in cases of dis-accreditation- *RAA 5.8*
✓	Streamline process of adding new gTLDs to accreditation – *RAA 3.1*
✓	Registrar responsibilities for acts of affiliates – *RAA 3.12*
✖	Staff to draft registrar code of conduct if registrars fail to do so by time certain

[6] In reading the chart: ✓ means has been addressed, x means the proposed amendment was not addressed either specifically or in total. Please note, however that, in relation to the reporting of data security breaches, Section 3.20 of the 2013 RAA now contains a requirement for Registrars to notify ICANN of the "unauthorized access to or disclosure of registrant account information or registration data". Further, and since the 2013 RAA has addressed all of the high/medium priority items except for the few noted, it was unclear whether a Code of Conduct was still needed, or what issues remained to be covered by such a Code. To the extent that the 2013 RAA mentions a Code of Conduct, this is not to be developed through a PDP (see Section 3.7.1 of the 2013 RAA).

VI. Treatment of Law Enforcement Recommendations in the 2013 RAA

The following chart summarizes the twelve LEA recommendations, indicates how they have all been addressed in the 2013 RAA, and lists the applicable section or specification in the 2013 RAA.

HOW THE 2013 RAA ADDRESSES LAW ENFORCEMENT RECOMMENDATIONS

	Summary of LE Recommendation	RAA Reference
1	Registrar duty to investigate reports of illegal conduct, including responding to reports from law enforcement, and providing a system to track complaints	• Section 3.18, requiring Registrars to maintain an abuse point of contact and provide a trackable system
2	Registrar shall not engage in activities or conduct that results in: (i) a conviction by a court of competent jurisdiction of a felony or other serious offense related to financial activities; (ii) a judgment by a court of competent jurisdiction that Registrar has committed fraud or breach of fiduciary duty; (iii) the Registrar being the subject of a judicial determination that is the substantive equivalent of those offenses (i)---(ii); or (iv) the Registrar knowingly and/or through gross negligence, permitting criminal activity in the registration of domain names or in the provision of domain name WHOIS information, after failing to promptly cure such activity after notice thereof.	• Section 5.5, which includes heightened and additional termination remedies
3	Registrar collection of data regarding registrations in addition to data already collected.	• The Data Retention Specification includes new items of data for retention and maintenance
4	Registrars abuse contact – posting of contact information and having a contact available around the	• Section 3.18, requiring Registrars to maintain an abuse point of contact
5	Publication of registrar information, including contact details, as well as regular updates to ICANN regarding changes in registrar business information	• Section 3.17.1 will now require registrars to provide updates to ICANN of the type of information that is required upon application for accreditation

6	Disclosure of affiliated registrars and affiliated businesses	• Section 3.17.1 (see item 5) incorporates this disclosure
7	Privacy and Proxy Services – Escrow, Reveal and Relay	• Section 3.14, regarding the development of an ICANN accreditation program • Proxy/Privacy Specification, putting in place interim requirements for proxy/privacy services offered through registrars
8	ICANN Accreditation of Proxy and Privacy Services	• See item 7.
9	Accountability of Resellers – Resellers must be held completed accountable to all provisions of the RAA.	• Section 3.12, imposing heightened obligations in relation to resellers
10	Registrar validation of registrant data	• Whois Accuracy Specification, setting out requirements for validation and verification of registrant and account---holder data
11	Whois service level agreements, with uptime minimums and specifying data update requirements.	• Whois SLA now includes these requirements
12	Expansion of grounds of termination of RAA for criminal convictions, including "knowingly and/or through gross negligence permit criminal activity in the domain name WHOIS information".	• Section 5.5, which includes heightened and additional termination remedies

VII. Next Steps in the Development of a Privacy Proxy Accreditation Program

In addition to the GNSO work on WHOIS issues, the ICANN Board passed a Resolution in November 2012 that addressed the recommendations from WHOIS RT's Final Report. As a result, ICANN has been actively implementing these recommendations in accordance with the Action Plan that was presented to the Board. In the Action Plan, ICANN committed to establishing a privacy/proxy accreditation program. The operational aspects of this new accreditation program will be conducted in parallel with the GNSO's RAA Remaining Issues PDP.

As part of this effort, in the coming months ICANN will examine its current registrar accreditation processes to determine how they might inform the development of the new privacy and proxy accreditation program. Issues to be explored in the implementation process include the type of due diligence to be conducted on privacy or proxy providers, the qualifications needed to become accredited, the contractual framework for establishing accreditation and appropriate oversight by ICANN, the types of enforcement or sanctions to be applicable in the event of breach, and addressing the escrow and data retention requirements, among others.

The chart below depicts those issues that have been raised by the ICANN community pertaining to privacy and proxy services that appear to be more appropriately addressed as part of the GNSO PDP. In addition to previous GNSO work on the issue, other recent recommendations that have focused on the topic that therefore might assist the WG in its deliberations have also been included where relevant. Please note that the chart is meant to assist the RAA Remaining Issues PDP WG in framing its work on the key aspects of privacy and proxy services as highlighted by previous community efforts. Since ICANN is committed to implementing the WHOIS RT recommendations per the Board's November 2012 Resolution, staff further recommends that the WG take these recommendations into account at an early stage in its deliberations.

Of note, the GNSO Council proposed a number of WHOIS-related studies in 2009 and 2010, which may help inform these deliberations. One such study, on WHOIS Proxy/Privacy Abuse, is being conducted by the

National Physical Laboratory (NPL) in the United Kingdom[7]. NPL's report is being finalized and is expected to be published for public comment shortly. Staff anticipates that NPL's findings will be published in time to be considered by the RAA Remaining Issues PDP WG during the course of its work.

ISSUE CHART FOR THE GNSO RAA REMAINING ISSUES PDP ON PRIVACY/PROXY SERVICES

	Issue	Explanation/Prior Recommendation	Source[8]	Policy Question to Be Explored
1	**Practices & Procedures**			
1.1	Standard 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	What are the types of Standard Service Practices that should be adopted and published by ICANN-accredited privacy/proxy service providers?
1.2	Standardized Relay and Reveal Procedures	Adopting agreed standardized relay and reveal processes and timeframes	WHOIS RT	What are the baseline minimum standardized relay and reveal processes that should be adopted by ICANN-accredited privacy/proxy service providers?
1.3	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	Should ICANN-accredited privacy/proxy service providers be required to reveal customer identities for this specific purpose?
1.4	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	Should ICANN-accredited privacy/proxy service providers be required to forward on to the customer all allegations they receive of illegal activities relating to specific domain names of the customer?

[7] See http://www.icann.org/en/news/announcements/announcement-2-18may10-en.htm.

[8] Excerpts from the source materials and relevant documents are included in Annex 1.

1.5	Revealing in instances of illegal malicious conduct	In instances of presentation 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	What forms of malicious conduct and what evidentiary standard would be sufficient to trigger such disclosure? What safeguards must be put in place to ensure adequate protections for privacy and freedom of expression?
1.6	Publication in WHOIS in instances of illegal conduct	Registrants using privacy/proxy registration services will have the contact information of the customer 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	What specific violations would be sufficient to trigger such publication? What safeguards or remedies should there be for cases where publication is found to have been unwarranted?

	Relationship with Customer			
2.1	Due Diligence	Conducting periodic due diligence checks on customer contact information (such as validation or verification of the same fields that are subject to validation or verification in WHOIS)	WHOIS RT	Should ICANN-accredited privacy/proxy service providers be required to conduct periodic checks to ensure accuracy of customer contact information; and if so, how?
2.2	Terminating a Customer's access	Cancel registrations of proxy services that do not fulfill their contractual obligations	WHOIS RT	What are the contractual obligations that, if unfulfilled, would justify termination of customer access by ICANN-accredited privacy/proxy service providers?

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	What rights and responsibilities should customers of privacy/proxy services have? What obligations should ICANN-accredited privacy/proxy service providers have in managing these rights and responsibilities? Clarify how transfers, renewals, and PEDNR policies should apply.

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	Should ICANN-accredited privacy/proxy service providers be required to label WHOIS entries to clearly show when a registration is made through a privacy/proxy service?
3.2	WHOIS Provider Contacts	Providing full WHOIS contact details for the privacy/proxy service provider, which are contactable and responsive	WHOIS RT	Should full WHOIS contact details for ICANN-accredited privacy/proxy service providers be required? What measures should be taken to ensure contactability and responsiveness of the providers?

4	**Abuse Point of Contact**			
4.1	Maintain Abuse Point of Contact	Maintaining dedicated abuse points of contact for each provider	WHOIS RT	Should ICANN-accredited privacy/proxy service providers be required to maintain dedicated points of contact for reporting abuse? If

				so, should the terms be consistent with the requirements applicable to registrars under Section 3.18 of the RAA?
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	What are the forms of malicious conduct that would be covered by a designated published point of contact at an ICANN-accredited privacy/proxy service provider?

5	**Law Enforcement**			
5.1	Access for Law Enforcement	The ability to hide ones identity in the global e-commerce marketplace creates and 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. There should be development of clear, workable, enforceable, and standardized processes to regulate access to registrant data when requested by law enforcement.	WHOIS RT	What circumstances would warrant access to registrant data by law enforcement agencies? What clear, workable, enforceable and standardized processes should be adopted by ICANN-accredited privacy/proxy services in order to regulate such access?

6	**Privacy Considerations**			
6.1	Balancing Privacy and Public Access	Consideration of use of domain name -- commercial v. personal, and whether the use of privacy or proxy services is	WHOIS RT	Should ICANN-accredited privacy/proxy service providers distinguish between domain

		appropriate when a domain name is used for commercial purposes		names used for commercial vs. personal purposes? Specifically, is the use of privacy/proxy services appropriate when a domain name is registered for commercial purposes? Should there be a difference in the data fields to be displayed if the domain name is registered/ used for a commercial purpose or by a commercial entity instead of to a natural person?
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	Should the use of privacy/proxy services be restricted only to registrants who are private individuals using the domain name for non-commercial purposes?

7	**Enforcement**			
7.1	Registrar to cancel Registrations	Registrar responsibility for cancellation under appropriate circumstances of registrations made by privacy/proxy services offered by others for noncompliance with Relay and Reveal	GNSO-ALAC RAA DT	What types of services should be covered, and what would be the forms of non-compliance that would trigger cancellation or suspension of registrations?

8	**General**			
8.1	Distinction between Privacy and Proxy Services	In considering Accreditation Program, take into account whether to distinguish between privacy/proxy services	WHOIS RT	Should ICANN distinguish between privacy and proxy services for the purpose of the accreditation process?

VIII. Conclusion

Given that this RAA Remaining Issues PDP is Board-initiated, with the publication of the Final GNSO Issue Report on the RAA on 6 March 2012 and the conclusion of the 2013 RAA negotiations, this PDP is now ready to move forward to the next stage. At this point in the process the next step for the GNSO Council will be to initiate the creation of a Drafting Team to develop a PDP Working Group Charter, form the PDP Working Group ("WG") and have the PDP WG commence its activities.

Staff recommends therefore that the GNSO Council proceeds to form a Drafting Team, to begin drafting a WG Charter taking into consideration the issues identified in this Report, the materials provided in Annex 1, and the relevant results of the Whois studies as published.

Given the number of identified issues related to privacy/proxy services, Staff further suggests that the Council may want to consider forming sub-teams within the PDP Working Group and/or separate the PDP into distinct parts. The Council may also want to consider publishing the list of proposed issues to be addressed in the PDP for public comment, to provide input for the Drafting Team and/or WG.

Finally, staff intends to share this Report with the Board for informational purposes and accordingly recommends that the Council inform the Board of its planned next steps.

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 study[9] 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. [10]

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:

[9] http://www.icann.org/en/compliance/reports/privacy-proxy-registration-services-study-14sep10-en.pdf

[10] 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/

privacy services have frequently frustrated our ability to protect our hotel brands online, which, unfortunately, often leads to confusion and other problems among consumers.[11]

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:

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.[12]

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.[13]

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.[14]

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).

---

[11] 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/

[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/

[13] 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/

[14] 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/

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'.

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.[15]

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.[16]

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.[17]

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

[15] 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/

[16] 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/

[17] 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

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 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.[18]
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.[19]

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:

[18] 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
[19] 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/

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:

ICANN should undertake to create an official set of guidelines for what constitutes a valid privacy/proxy service and best practices for such services.[20]

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.[21]

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:

[20] 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/

[21] 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.[22]

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.[23]

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.[24]

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 and 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.[25]

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.[26]

---

[22] 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/

[23] 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/

[24] 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/

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

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

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**	Conspicuous Notice- "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." -- eliminate this clause		Priority: High
5.2	**Registrars to list privacy/proxy services offered and description of services**	**3.4.1**	**Staff**		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 to escrow of Whois	Priority: High (disclosure obligation)

					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	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.		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. Priority: Low

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**	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, and administrative contact information." Lastly, proxy and privacy registrations contravene the 2007 GAC Principles on WHOIS.		Priority: Low

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

VI. Excerpts from the 2013 RAA:

3.4 Retention of Registered Name Holder and Registration Data.

3.4.1 For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:

…

3.4.1.5 the name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program.

3.12 Obligations Related to Provision of Registrar Services by Third Parties. … In addition, Registrar must ensure that:

…

3.12.4 Its Resellers comply with any ICANN-adopted Specification or Policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a “Proxy Accreditation Program”). Among other features, the Proxy Accreditation Program

may require that: (i) proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities Accredited by ICANN pursuant to such Proxy Accreditation Program; and (ii) Registrar shall prohibit Resellers from knowingly accepting registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, Registrar shall require Resellers to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.14 Obligations Related to Proxy and Privacy Services. Registrar agrees to comply with any ICANN-adopted Specification or Policy that establishes a Proxy Accreditation Program. Registrar also agrees to reasonably cooperate with ICANN in the development of such program. Until such time as the Proxy Accreditation Program is established, Registrar agrees to comply with the Specification on Privacy and Proxy Registrations attached hereto.

REGISTRAR INFORMATION SPECIFICATION

Registrar shall provide to ICANN the information specified below, which shall be maintained in accordance with Section 3.17 of the Agreement. With regard to information identified below, ICANN will hold such information pursuant to the disclosure requirements set forth in Section 3.15 of the Agreement.

…

Other

23. Does the Registrar or any of its Affiliates offer any Privacy Service or Proxy Service (as such terms on defined in the Specification on Privacy and Proxy Registrations)? If yes, list the entities or individuals providing the Privacy Service or Proxy Service.

SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS

Until the earlier to occur of (i) January 1, 2017, and (ii) the date ICANN establishes and implements a Privacy and Proxy Accreditation Program as referenced in Section 3.14 of the Registrar Accreditation Agreement, Registrar agrees to comply, and to require its Affiliates and Resellers to comply, with the terms of this

Specification, provided that ICANN and the Working Group may mutually agree to extend the term of this Specification. This Specification may not be modified by ICANN or Registrar.

1. Definitions. For the purposes of this Specification, the following definitions shall apply.

   1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.

   1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Service (Whois) or equivalent services.

   1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (Whois) or equivalent services rather than the P/P Customer's contact information.

   1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

2. Obligations of Registrar. For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates must require all P/P Providers to follow the requirements described in this Specification and to abide by the terms and procedures published pursuant to this Specification.

   2.1 Disclosure of Service Terms. P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.

   2.2 Abuse/Infringement Point of Contact. P/P Provider shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).

   2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.

2.4 Terms of service and description of procedures. The P/P Provider shall publish on its website and/or Registrar's website a copy of the P/P Provider service agreement and description of P/P Provider's procedures for handling the following:

2.4.1 The process or facilities to report abuse of a domain name registration managed by the P/P Provider;

2.4.2 The process or facilities to report infringement of trademarks or other rights of third parties;

2.4.3 The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer;

2.4.4 The circumstances under which the P/P Provider will terminate service to the P/P Customer;

2.4.5 The circumstances under which the P/P Provider will reveal and/or publish in the Registration Data Service (Whois) or equivalent service the P/P Customer's identity and/or contact data; and

2.4.6 A description of the support services offered by P/P Providers to P/P Customers, and how to access these services.

2.5 Escrow of P/P Customer Information. Registrar shall include P/P Customer contact information in its Registration Data Escrow deposits required by Section 3.6 of the Agreement. P/P Customer Information escrowed pursuant to this Section 2.5 of this Specification may only be accessed by ICANN in the event of the termination of the Agreement or in the event Registrar ceases business operations.

3. Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:

3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;

3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or

3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

Registrants' Benefits and Responsibilities

Domain Name Registrants' Rights:

1. Your domain name registration and any privacy/proxy services you may use in conjunction with it must be subject to a Registration Agreement with an ICANN Accredited Registrar.

   - You are entitled to review this Registration Agreement at any time, and download a copy for your records.

2. You are entitled to accurate and accessible information about:

   - The identity of any proxy or privacy service provider affiliated with your Registrar;
   - Your Registrar's terms and conditions, including pricing information, applicable to domain name registrations;
   - The terms and conditions, including pricing information, applicable to any privacy services offered by your Registrar;
   - The customer support services offered by your Registrar and the privacy services provider, and how to access them;
   - How to raise concerns and resolve disputes with your Registrar and any privacy services offered by them; and
   - Instructions that explain your Registrar's processes for registering, managing, transferring, renewing, and restoring your domain name registrations, including through any proxy or privacy services made available by your Registrar.

3. You shall not be subject to false advertising or deceptive practices by your Registrar or though any proxy or privacy services made available by your Registrar. This includes deceptive notices, hidden fees, and any practices that are illegal under the consumer protection law of your residence.