The ICANN GNSO "Business Constituency"

Comments on Initial Report from the Expert Working Group on gTLD Directory Services

Status: FINAL

Version: 4

6-Sep-2013

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the feedback of the ICANN Business Constituency (BC). The BC's comments arise from the perspective of Business users and registrants, as defined in our Charter[1]:

The mission of the Business Constituency is to work for policy that fosters an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business;
2. is competitive in the supply of registry and registrar and related services; and
3. is technically stable, secure and reliable.

ICANN's Expert Working Group on gTLD Directory Services (EWG) recently issued an Initial Report to share its review, analysis and recommendations for the Next Generation Registration Directory Service[2].

In the report, the EWG recommends a centralized, purpose-driven system called the Aggregated Registration Directory Service (ARDS) model. The EWG has conducted webinars and public sessions in July 2013, and is currently asking for community input on the Initial Report, as well as on a number of questions that remain unresolved and under discussion within the EWG.

The BC offers two general comments, followed by specific answers to EWG questions.

General Comment #1: *Benefits of Centralized RDS data are clear, but ICANN Must Manage the Risks*

The BC has long recognized the benefits of a centralized RDS that provides accurate and readily available registration data to individuals and organizations with legitimate interest in accessing the information. In our 2011 "*Response to WHOIS Policy Review Team Discussion Paper*", we said, "ICANN should also consider mechanisms to create and maintain a centralized WHOIS database, as referenced in the RAA."[3]

At the same time, the BC also sees increased security risks with a centralized data model, as the EWG recognized on page 3 of its report:

- Creation of a "Big Data" source of highly valuable data with potential for misuse if not properly audited and maintained.
- Increased risk of insider abuse and external attack, requiring greater attention to security policy implementation, enforcement and auditing

Some BC members believe the risks of centralization could outweigh the benefits. Therefore, the BC supports continued exploration of centralized ARDS, along with a deliberate and detailed study of potential security risks and recommended mitigation plans, most likely involving the SSAC.

[1] Business Constituency Charter, at http://www.bizconst.org/charter.htm.

[2] Initial Report from the Expert Working Group on gTLD Directory Services: A Next Generation Registration Directory Service, 24-Jun-2013, https://community.icann.org/display/WG/Explore+the+Draft+Next+Generation+gTLD+Directory+Services+Model.

[3] BC Comments on WHOIS Policy Review Team, 23-Jul-2011, at http://www.bizconst.org/Positions-Statements/BC_on_WHOIS_Review_Questions.pdf

General comment #2: *Eligibility for "protected registrants" and obligations for protection providers.*

The BC supports the EWG concept of "permissible purposes" for access, which include priority BC uses such as "Legal Action" and "Abuse Mitigation" to protect business registrants and users. At the same time, the BC supports the EWG proposal to accommodate registrant Privacy, as described on page 3: "*the EWG recognizes the need for accuracy, along with the need to protect the privacy of those registrants who may require heightened protections of their personal information*."

However, the EWG has not yet defined eligibility criteria for "protected registrants", and must address obligations of privacy/proxy services when they are presented with evidence of actionable harm. Each of these challenging questions are addressed below:

Eligibility for protected registration

Eligibility for privacy/proxy protection should only be extended to registrants who promise not to solicit sales, payments, or donations, and promise not to facilitate infringement of intellectual property rights, distribution of malware, phishing, or other fraud.

And the EWG's "Maximum Protected Registration" should only be available to registrants who demonstrate a need for privacy to protect at-risk free-speech uses.

Both these questions of eligibility should be further explored by the EWG, with plenty of community input. Once the EWG develops eligibility criteria for privacy protection services, the community can discuss implementation. For example, a self-designation method might need a method of verification and revocation of the proxy/privacy protection if there is abuse by the registrant.

Much has already been discussed about the need for anonymity in certain situations. Someone wanting to exercise their right of free expression can use a platform where the individual is not the domain registrant (e.g.: Wordpress). In addition, there are cooperative projects designed to allow political dissidents to remain anonymous. See www.torporject.org for an excellent example of such efforts.

Obligations of privacy/proxy services

Even where registrants are deemed eligible for privacy/proxy protection, the BC restates our Jun-2012 comment on *WHOIS Affirmation Review*, where we agreed that privacy/proxy services should:

- Adopt agreed standardized relay and reveal processes and timeframes
- Conduct periodic due diligence checks on customer contact information
- Provide clear and unambiguous guidance on the rights and responsibilities of registered name holders, and how those should be managed in the Privacy / Proxy environment

In our May-2013 comments on the new RAA, the BC held that privacy/proxy services must be obliged to relay and/or reveal registrant information when presented with evidence of actionable harm or abuse[4]:

- Specify under what circumstances, pursuant to section 2.4.3, the P/P Provider will relay communications from third parties to the P/P Customer. The BC recommends that the P/P Provider be required at a

[4] page 3, BC Comments on Proposed Final Registrar Accreditation Agreement (RAA), May-2013, at http://www.bizconst.org/Positions-Statements/BC%20Comment%20on%20final%202013%20RAA%20%5BFINAL%5D.pdf

minimum to relay any communications alleging illegal conduct or consumer fraud (e.g., infringement of intellectual property rights).

- Specify under what circumstances and which time frame, pursuant to section 2.4.5, the P/P Provider will be required to reveal the Whois information of the P/P Customer. The BC recommends that if illegal activity is alleged, that the P/P Provider be required to reveal the Whois information and that this revelation occurs within seven (7) business days to conform to section.

The BC continues to maintain these prior positions regarding obligations of privacy/proxy services. This is based on our members' extensive experience responding to abusive registrations and illegal activity on domains, where the actual registrant was using privacy/proxy to avoid or delay accountability.

BC Responses to Specific Questions from the EWG

Regarding the EWG's suggested Aggregated RDS model, are there additional advantages and disadvantages that should be considered? In such a model, which data repository (ARDS or Registry) should be considered authoritative?

As stated above, the BC is generally in favor of the ARDS model. The BC recognizes that there are several advantages to the ARDS, such as the ability to provide data in a consistent format, pursuant to a consistent process, which can streamline the efforts of the consumers of registration data, thereby lessening the burden on rights holders and law enforcement, among others.

Another advantage of the ARDS model is the likelihood that ICANN can better manage compliance to community-approved rules and regulations for the ADRS. ICANN can also better assess the integrity of registrant data (completeness and accuracy of registrant records) as a single audit of a single database is likely much easier and possibly much less expensive than multiple audits of multiple databases.

Abuse of a single, purpose-driven database would also be much easier to prevent, and track. Bulk access to registration data would be restricted to those with legitimate and verified purposes, which could reduce the number of individuals and entities who compile that information for spam or other "miscreant" behavior. If an individual or entity uses the information for spam or other forms of abuse, a centralized ARDS model seems to lend itself to quick identification and punitive action.

Some have criticized the centralized ARDS model as likely to be "too big" and therefore vulnerable to either technical failure or malfeasance.

The BC recommends that ICANN Board request further study and recommendations, perhaps via a report guided by the SSAC, on this point. However we do note that the registry data repository, which the BC believes should be considered authoritative, will retain ultimate control of registrant records so in the unlikely event of data loss or breach, data can be reassembled/recreated. The BC believes that overall it will likely be safer to centralize the data than to leave data distributed across multiple individualized databases, many with untested security. A further concern that the BC has raised in the past is the difficulty for legitimate

WHOIS users to utilize a directory service that is distributed across hundreds to thousands of registrars and registries, in the post new gTLD launch, for instance.

Could the EWG's recommendation for purpose-driven authenticated Gated Access to validated registration data satisfy identified RDS users and their needs? In such a model, how would requestors be identified, authorized and issued RDS access credentials? In particular, who would accredit law enforcement agents, based on what criteria?

The BC appreciates the challenge facing the EWG and the ICANN Community, to develop appropriate mechanisms for the validation of credentials necessary to obtain Gated Access to registration data. The BC suggests that requestors can submit their qualifications to a third party, funded or subsidized by ICANN, to be approved on the basis of secure, protected credentials.

Corrective measures should be in place to withdraw or cancel Gated Access if the requestor abuses the system or misrepresents their purpose to the validator.

The BC recognizes the unique challenge as this relates to individuals exercising freedoms that are consistent with international treaties and the rights of others and are established in democratic societies but are nonetheless being pursued for prosecution and their identify is being obtained via Gated Access.

There is also a concern that an aggregated data contact list relating to law enforcement professionals could also be subject to both misuse and attack. Coupled with a global directory for Gated Access, this could present significant operational challenges if, for example, a coordinated attack or temporary downtime prevented security professionals from accessing information necessary to counter fraud and other malfeasance. Again, we would recommend that SSAC undertake a risk assessment of these potential issues.

Could the EWG's recommendations for addressing maximum protected registration satisfy both accountability needs and the privacy needs of at-risk individuals? How might a suitable solution be identified and funded?

Please see general comment #2 above, regarding the balance between accountability and privacy.

Are the users and purposes identified by the EWG thus far sufficiently representative? Are there any significant gaps in users and purposes that must be addressed?

The BC appreciates that the EWG faces a very difficult task in anticipating all the possible use cases for the ARDS service and developing access models for each. We think the initial report is an admirable starting point. We ask that the EWG continue to solicit ideas and feedback from the ICANN community, and that the ARDS model will be open to inclusion of more use cases as they are discovered and explored.

We recognize and support the development of a comprehensive system, including in particular, accreditation of privacy and proxy services, to restrict privacy and proxy use to legitimate

purposes and not as a shield that encourages abuse on the Internet. Accreditation of privacy and proxy services should take into account, the exercise of freedoms and the protection of political speech/activity in our general comment above.

Given the desire for an extensible next-generation RDS that might accommodate the needs of a rapidly-evolving global Internet, how could future new users and purposes be accommodated? Who would decide on permitted purposes, using what criteria?

The BC believes that future new users and purposes can be created upon request of the new group that seeks access. Whatever third-party validation system is developed can easily accommodate a new use/purpose, if verified in accordance with the existing policy.

As with changes to other ICANN implementation mechanisms, any requests can be published for public comment, and any concerns of the community can be addressed before permitting the new use.

Are the registration data elements identified by the EWG thus far sufficiently representative of the data required for each identified purpose? Are there any significant gaps in data elements that must be addressed?

The BC supports the work of the EWG thus far to identify the appropriate data elements required to address each identified purpose. Consistent with our general comments above, the BC encourages the EWG to ensure that sufficient elements required for identification of registrants who are soliciting payments or donations are available to all potential customers, donors, and users of these services.

How should public and gated data elements be classified? What criteria should the EWG apply to make initial recommendations in this area?

Consistent with our general comments above, the BC believes that sufficient data elements required for identification of the registrants who run commercial services should be available to all potential donors, users, and consumers of these services. The BC urges the EWG to consider the criteria proposed above to develop recommendations regarding various categories of registrants, such as commercial and non-commercial, etc.

What community needs should be considered during the EWG's discussion of registration data storage duration, escrow and access log requirements?

The primary community concerns regarding data storage duration, escrow and access log requirements are: the needs of law enforcement to access information, the needs of intellectual property rights holders, concerned parties who are accessing a website and wish to verify that it is a legitimate site; which might include parents, citizens who are seeking content from a website and are concerned about who operates it; the need for privacy in legitimate circumstances, the need to prevent spam or other abuse of registrant information, and the need to comply with local and international laws.

The EWG acknowledges that deploying and operating the suggested RDS will incur costs. In such a system, how could or should these costs be borne?

> Cost recovery for an ARDS model should be split amongst the various groups that benefit from the centralized system. The Registries, for example, could pay a small fee per record as the centralized database is a backup for them. Entities accessing the data could pay a fee for retrieving Gated Access information, which could be done as an upfront cost paid at the time of certification/validation or per request. ICANN could also underwrite the validation/certification costs for Gated Access.
>
> The BC believes however, that for domain names use for commercial purposes, as defined and discussed above, basic data elements which identify the registrant should be available to Internet users and consumers without a fee. Additional data elements might require a fee, however these fees should be limited to recovery of actual costs.

As final comment, the BC believes that a unified model for all registration data, regardless of whether that data is for the generic or country code namespaces, would best serve Internet users. Although the BC understands that the cc space is out of scope of the EWG's current work, we hope that the drive to unify registration data at generic level may lead to the same type of approach for the cc community.

These comments were prepared in accordance with the BC Charter, with wide participation by BC members. Laura Covington prepared the initial draft. The final version was approved by membership on 6-Sep-2013.