April 10, 2019

IPC and BC Comments on the TSG Draft Technical Model

The GNSO Intellectual Property and Business Constituencies (the IPC and BC) welcome this opportunity to provide comments to the Technical Study Group on Access to Non-Public Registration Data (the TSG) on the TSG's Draft Technical Model for Access to Non-Public Registration Data (the Model).[1] At the outset, we wish to thank the members of the TSG for their efficient and exhaustive work on the Model – which, as the IPC publicly noted at ICANN64 in Kobe, has already "added both substantive value and efficiency in working towards the goal of a unified access model."[2] We further agree with the TSG that the Model achieves its stated purpose – namely, to propose a technical solution for access to non-public domain name registration data in gTLDs[3] – in a manner that is consistent with the dual motivations of the TSG: 1) to balance data protection requirements with legitimate interests of third parties to access non-public gTLD registration data; and 2) to reduce the potential liability faced by gTLD registries and registrars when providing such access.[4] With respect to the latter, the TSG has repeatedly noted that one overarching objective of its work on the Model was to design a technical solution by which ICANN could attempt to reduce the GDPR liability of registrars and registries.[5] We appreciate that objective, and appreciate the work of the TSG toward achieving it.

Notwithstanding its overall support for the Model, the IPC and BC offers the following comments and suggestions on specific elements of it.

Section 4 – Use Cases

Use Case #1 (Critical) states that "Reverse search capabilities are contemplated, but the TSG recognized that this is an advanced search capability that is not fully supported at this point in time". Given the importance of this functionality in abuse investigations, we believe that ICANN and the IETF community should continue to actively pursue and complete the standardization of mechanisms to implement

---

[1] *See*: https://www.icann.org/en/system/files/files/draft-technical-model-access-non-public-registration-data-06mar19-en.pdf.

[2] *See* https://static.ptbl.co/static/attachments/201328/1552521431.pdf?1552521431 at 7.

[3] Model at 1.

[4] *See*: "ICANN64 – Community Engagement Session: TSG on Access to Non-Public Registration Data Presentation Slide Deck" at https://www.icann.org/en/system/files/files/presentation-tsg-access-rd-11mar19-en.pdf (the "Deck") at 4.

[5] *See, e.g.*, Deck at 8; *see also, e.g.*, https://static.ptbl.co/static/attachments/202980/1553546750.pdf?1553546750 at 132 (". . . . [T]he whole venture is to reduce the risks attendant on the registrars and registries with respect to GDPR liability.").

reverse lookup capabilities (currently defined in Internet Draft https://datatracker.ietf.org/doc/draft-ietf-regext-rdap-reverse-search/). While we understand there is a privacy concern related to these features, the privacy policies and eventual access mechanisms being developed in ICANN to ensure access is limited to properly accredited entities sufficiently addresses these concerns. In addition, reverse searching capabilities could be designed in a manner to minimize privacy concerns, such as identifying a domain name associated with the specific data field that is being searched (such as an email address).

Section 4.1 – User Journey

The user journey outlined in this section does not seem to represent the user journey of a typical RDS user. We suggest that additional context and descriptive text be added to this section to ensure it is clear to the reader what "journey" is being described and why it is relevant. In addition, we suggest that this section should be framed from an RDS users' point of view. Finally, we do not understand what bullet #2 ("Correlate based on different aspects….") is describing as it is not clear how any correlation can be achieved without access to the underlying data. Perhaps additional context (and improved wording) would help in this regard.

Section 5 - System Requirements

The "ICANN RDAP Gateway" requirements described in item 4.e and 4.f seem to blur the lines between policy definition and implementation. We suggest that these requirements be conditional on the TBD policy. E.g.

> e. If future policy dictates that requestor *attributes* be passed to the authoritative contracted party RDAP server, the system MUST support the inclusion of requestor *attributes* (see 2.b) in the RDAP message from the ICANN RDAP Gateway to the contracted party RDAP server.

> f. If future policy dictates that requestor *identifier* be passed to the authoritative contracted party RDAP server, the system MUST support the inclusion of requestor *attributes* (see 2.f) in the RDAP message from the ICANN RDAP Gateway to the contracted party RDAP server.

Requirement 4.h "The system MUST enable automation of client requests." sounds important but to the average reader it is not clear what this means. Additional context should be added.

Section 7 – Actor Models

We believe that Actor Model 2 is the best fit given the assumptions, use cases and system requirements described earlier in the document.   If the TSG has agreement as to which model should be considered moving forward, we suggest it be explicitly stated in this section.

Section 9 – Proposed Solution

The second paragraph states "Mutual TLS authentication will be used to secure RDAP communications between ICANN and the Contracted Parties, and also between subsystems." Given the RDAP RFCs indicate that support for Mutual TLS authentication is OPTIONAL we note that a future RDAP profile will need to indicate this feature is MANDATORY.

Section 9.1 – Prerequisites

It is not clear what "Identity Providers, third party authorizers, and ICANN must exchange configuration information to identify service endpoints." Means and suggest that additional context and clarity be added describing what problem this "prerequisite" solves and how.