ICANN Business Constituency

Comment Regarding ICANN's Proposed Unified Access Model

13-Sep-2018

Thank you for the opportunity to comment on ICANN's proposed Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data (UAM)[1].

As is well known, members of the Business Constituency (BC) have been active in proposing elements of an Accreditation and Access Model (AAM)[2]; while the BC does not agree with every aspect of the UAM, we support and are pleased to see an expanding and productive discussion about a consistent and predictable way for third parties to access full registration data.

Timelines

The BC thanks ICANN Org for advancing the discussion of a unified access solution for non-public Whois data for lawful and legitimate purposes, and for acknowledging the harms that many in the community are facing without an access model in place.

While we appreciate that ICANN Org has introduced a draft access framework for discussion, the need for access has become more acute since May-2018 and necessitates rapid action instead of slow-paced discussion. We therefore reiterate that ICANN should act in the public interest by expeditiously pushing forward for a temporary unified access solution for security, law enforcement, consumer protection and intellectual property needs, while the community works to develop a permanent solution via the EPDP.

ICANN Org should accordingly prioritize this matter more highly, including facilitation of a more detailed community process to move the model forward, production of developmental milestones and a timeline for reaching agreement, and adoption of a temporary specification to implement it.

Comment on the UAM

Purpose of the paper (Sec. A, Introduction)
ICANN states that the purpose of the paper is to:

> *…facilitate further discussions with the European Data Protection Board and the ICANN community about a unified access model.*

The BC refers ICANN Org to the above section on timelines. While discussion is appreciated, action toward a defined outcome must be the priority.

---

[1] See https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf

[2] Draft Accreditation and Access Model for Non-public Whois Data (v1.7), at https://mm.icann.org/pipermail/accred-model/attachments/20180720/8d8c713f/DRAFT-WHOISAccreditationandAccessModelv1.7-0001.pdf

Brief Summary of the Framework (Sec. B)
ICANN writes in Section B that:

> *…a third party that is part of an "eligible user group" could submit an application to an "accrediting body" to apply for credentials to be used to access non-public WHOIS data.*

The BC concurs.

> *…the user would be required to agree to abide by Terms of Use that would include required measures to adequately safeguard the personal data that may be made available to the user. Violation of the Terms of Use could result in revocation of the user's credentials for access among other things.*

The BC concurs with this as well.

> *To make a specific query for a domain name the user would take its credentials to the relevant registry operator or registrar to perform a query through an RDAP service.*

The BC agrees that RDAP is expected to be the technical basis for any such service.

> *As part of its query, the user would be required to specify its purpose for accessing the data…*

The BC agrees, though it would be over-burdensome to make purpose specification mandatory for each individual record. There will be times when efficiency must prevail, allowing users to specify a purpose for the lookup of multiple records at once.

> *The registry operator/registrar would validate the credentials with the authenticating body before providing a response to the user's query.*

The BC needs to hear more about this potential step before providing input.

Community Views About High-Level Elements of a Unified Access Model (Sec. E)

ICANN's discussion in Section E highlights areas where there is convergence on key elements of a possible model, including:

- Using RDAP;
- Implementing strong safeguards; and
- Using a decentralized process for developing criteria and methods for authenticating various types of users.

The BC supports the above three elements.

ICANN further writes that there are competing views on the legal requirements of GDPR as they related to the model:

1. *Whether or not an authenticated user requesting access to non-public WHOIS data must provide its legitimate interest for each individual query/request;*

As stated above, the BC finds it over-burdensome to make purpose specification mandatory for each individual record. There will be times when efficiency must prevail, allowing users to specify a purpose for the lookup of multiple records at once.

2. *Whether or not full WHOIS data must be returned when an authenticated user performs a query;*

The BC believes the full record should be returned.

3. *Whether or not logs of query activities concerning non-public data must be available to the registrant upon request except if prohibited by a relevant court order or legal requirement.*

The BC urges the community to take particular care in consideration of how, or if, logged access data is collected and used publicly. As has been pointed out by many as an example, criminal elements could use this information to determine whether or not they're under investigation, hampering law enforcement efforts. Further, we support ICANN's ongoing consideration about whether or not logging a requestor's personal data violates GDPR.

4. *Whether or not both registrars and registry operators must be required to provide access to non-public registration data;*

The BC believes both registry operators and registrars must provide data. However, we also find merit in the idea of an RDAP portal operated by ICANN that can handle and vet requests.

5. *Whether or not there should be a fee imposed for accessing non-public WHOIS data;*

The BC favors a yearly fee for accreditation of data users, but not a fee for accessing the data.

6. *Whether or not there should be a centralized portal operated by ICANN from which authenticated users are able to perform queries of non-public WHOIS data.*

   The BC believes this option could be more consistent, predictable, and expedient for users. Accordingly, the BC encourages ICANN to immediately explore technical and legal implications of this option. At the first opportunity, ICANN should explain this option to the EU Data Protection Board and seek their guidance about whether this approach is acceptable.

   However, while exploring this option, ICANN must provide clear rules that ensure contracted parties immediately begin to provide "reasonable access" for purposes of cybersecurity, law enforcement, consumer protection, and intellectual property protection.

Feedback on Summary Description of a Framework for a Possible Unified Access Model (Sec. F)

The BC provides here feedback on areas of concern or disagreement, ordered according to the relevant questions posed in the summary description.

1. *Who would be eligible for continued access for WHOIS data via a unified access model?*

ICANN indicates here that "Only a defined set of user groups with legitimate interests who are bound by Terms of Use requiring adequate measures of protection would be eligible for access to non-public WHOIS data via a unified access model."

The BC concurs, with the following caveat: It depends on how a user group is defined. Our position is that user groups may in fact self-define, present legitimate purposes, and request access. A user group need not wait to be identified and validated by another party -- should it have legitimate purposes for WHOIS data, it should approach the accreditation authority for access.

2. *Who would determine eligibility?*

ICANN envisions that, "At the outset governments within the European Economic Area (who are also members of the GAC) would identify or facilitate identification of broad categories of eligible user groups."

The BC disagrees. The GAC is on-record saying it, "does not envision an operational role in designing and implementing the proposed accreditation programs…"[3] Nor, do we believe, is the GAC suited for such a role. Further, the BC respectfully points out that while GDPR is a European law, the UAM would not be driven solely by GDPR. It therefore makes little sense to limit initial "approvers" to the governments of the EEA.

The BC is concerned with the possibility of delay and confusion involved in having governments "pick winners" for access. The need for a credible access program is acute, and is growing more so by the day. It's critical that the envisioned access model be moved expeditiously toward implementation, without needless restrictions.

3. *How would authentication requirements for legitimate users be developed?*

According to the UAM, "For private third parties, ICANN would consult with the GAC and members of the Eligible User Groups to identify relevant bodies with expertise to authenticate users within an Eligible User Group (the "Authenticating Bodies"), and the Authenticating Bodies would develop criteria to authenticate individual users within an Eligible User Group."

The BC reiterates that governments are unlikely to be interested in an operational role with regard to the model. However, the BC agrees that authentication should be assigned to bodies with appropriate expertise.

5. *What would be the overall process for authenticating legitimate users for access (sic) non-public WHOIS data under a unified access model?*

[3] https://gac.icann.org/contentMigrated/icann61-san-juan-communique

ICANN poses a question toward the end of its answering paragraph: "There is a question about whether the authenticated user would be required to enter into some type of "access" agreement with the registry operator or registrar above and beyond the Terms of Use."

The BC believes this is burdensome and unnecessary. Mandatory terms of service, including a global "access policy," as part of the accreditation process would suffice.

6. *What scope of data would be available to authenticated users?*

ICANN writes: "This paper takes the position that access to non-public WHOIS data would be on a query-by-query basis, and that it would not be permissible to provide the full WHOIS record by default to an authenticated user, unless doing so would be supported by the legitimate interest provided by the authenticated user."

While the BC supports a legitimate requestor being given access to the full registration record, in any scenario where only a limited number of redacted fields are returned to the requestor, more clarity is required regarding how the decision to do so is made.

For example, a security researcher may be attempting to contact the owner of a compromised website but, in a WHOIS data request, the registrar returns only an email address. If the email elicits no response, can the requester ask for the phone number? Doing so also suggests a process that is unnecessarily burdensome and elongates the time to remediation.

8. *Would a unified access model incorporate transparency requirements?*

The BC is pleased to see transparency requirements included in the design of the UAM. However, we disagree with making audit logs available to registrants for the reasons stated above.

ICANN further states, in the final paragraph of the section: "…it is not clear that searchable WHOIS functionality for non-public WHOIS data would be consistent with these accountability requirements of the GDPR. ICANN org proposes to seek further guidance from the European Data Protection Board on this matter to better understand what may be permitted."

The BC supports full consultation with the EDPB in this regard, as this is an important capability in light of the needs of the security, law enforcement and IP communities.

16. *How would the Terms of Use be developed?*

The BC encourages ICANN org not only to consult with the GAC and EDPB, but the community as well.

17. What types of safeguards would be included in the Terms of Use?

ICANN refers to rate limiting at the end of this section, stating that it is undecided about rate limiting and needs to further discuss the matter with the community. The BC is opposed to rate limiting, as it indeed handcuffs the work of investigators, security researchers, and others who rely on timely access to records.

Specific document redlines

Page 2: Section B
The BC suggests that the beginning of section B (at (1)) should also discuss the collection of data as well as data access.

Page 4: Section B
The text about Attachment 1 mentions questions that arise for "registry operators/registrars, the authenticating bodies, and ICANN." The user should also be represented here. There are many questions from the user perspective, who is a relevant actor in this process. As such, Attachment 1 also needs to be modified to include a column for the user. By way of example, a question about the accreditation request process could be "how long should the user expect to wait to receive word on the success of their application?"

Page 8: Section F(1)
Once again, the term "reasonable access" needs to be defined.

Page 8: Section F(1) Paragraph 2
The BC recommends striking this entire paragraph. The current default solution (Temp Spec) protects the rights of individuals. The entire point of the UAM is to provide a way for third parties with legitimate interest to access the data. So, establishing who those eligible third parties may be is primary to the process.

Page 14: Section 14
This requires more clarity. Who, for example, are authorized third parties that an accredited party can forward WHOIS data to? Law enforcement? Other accredited entities? This question is even more pertinent when we consider "proxies" for end users. Can attorneys or a brand-focused registrar make a request on behalf of a user and pass along the data?

Page 15: Section 17(b)
Why is there a need for query limits in a regime where, currently, only single requests are allowed at a time?

Attachment 2
More clarity is required regarding how Steps 3 and 4 work, and specifically why these can't be combined into one step. If the user is submitting all the data, including the domains in question and the legitimate purpose, the registrar can just return the data rather than simply confirming the accreditation and the legitimate interest and then creating some mechanism for the user to then go elsewhere to do a query for just the information they are allowed to query for? This is burdensome.

--
This comment was drafted by Mason Cole, Tim Chen, and Margie Milam, with edits by Steve DelBianco.

It was approved in accord with our Charter.