ALAC Statement on “Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data”

Greg Shatan

ICANN 63
21 October 2018

Prior ALAC Statement regarding Access

- 10 April 2018, ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model,"
- Impractical and unreasonable to require third-parties with a clear legitimate interest to obtain a court order to be granted access to non-public WHOIS data on a case-by-case basis.
- ALAC agrees with proposal that user groups with a legitimate interest and who are bound to abide by adequate measures of protection should be able to access non-public WHOIS data based on explicit pre- defined criteria and limitations under a formal accreditation program.
  - Method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR.
- Engagement with EU DPAs to define and reach agreement on an accreditation approach is critical.

General Comments

1. Any "access model" must be compliant with GDPR.
   - ICANN must seek and receive legal advice on compliance from qualified counsel.

General Comments

2. Rights and concerns of end-users must always be part of any calculus

- End-users are the most numerous participants, and the most likely to be harmed by abuse and other violations.
- Email recipients should have the right to find out “who is” sending them e-mail.
- Website users should have the right to find out “who is” behind a website.
- Mail service providers should have the right to find out “who is” using their resources to determine if they are spammers.

General Comments

3. Access model must be designed to be scalable and perform at scale.

- Abuse moves at automated speeds
- An agreed-upon set of inputs and outcomes will enable automated systems for WHOIS information requests in an appropriate and consistent fashion.

General Comments

4. The various harms must be balanced in a non-biased fashion.

- Various scenarios should be approached dispassionately and scientifically.
  - This area can become an ideological minefield, which in turn tests the multistakeholder model.
- More balanced and detached approach more likely to lead to solid guidance, consistent decision-making and realistic implementation.

Eligibility

1. Who would be eligible for continued access for WHOIS?

- **Summary of Framework Response**: The proposed UAM would be open to a "defined set" of "user groups" with "legitimate interests."
  - Attempts to strike balance between third parties with legitimate interests who may regularly request access "where additional safeguards and process may be required or warranted" and other third parties who request access more rarely.
- ***Comment****: ALAC supports this aspect of the UAM, but:*
  - *Framework is very short on specifics.*
  - *Developing this list of "user groups" will be a critical element in the development of the UAM.*
- *Whether third parties should be able to appoint representatives to request and receive access on their behalf (e.g., an investigator or an attorney) requires further exploration*
  - *How representatives be validated or authenticated,*
  - *How to be reasonably certain representative is bona fide.*
  - *Terms of Use could cover these issues.*
  - *Access system should not be set up to favor or disfavor certain user types.*

2. Who would determine eligibility?

- **Summary of Framework Response:** GAC members in EEA would identify or “facilitate identification” of broad categories of “Eligible User Groups.”
  - ICANN org would engage with other governments through GAC to identify specific Eligible User Groups.
- ***Comment:*** *ALAC prior comment: “believes that the accreditation mechanism to be applied should be developed by the entire community, in a true multistakeholder fashion. … The ALAC doubts whether the GAC should be given such a – seemingly – prominent role to establish … what the criteria for accreditation should be. Again, this should be a multistakeholder process.”*
- *The ALAC reiterates these views.*
  - *Most Eligible User Groups are likely to be non-governmental in nature.*
  - *Governments do not possess any special expertise or knowledge in identifying such Eligible User Groups*
    - *Ceding such a vital aspect of the process to governments sets a bad precedent for ICANN as an organization “rooted in the private sector.”*
  - *Need to balance various stakeholder sectors. If there is a geographic or jurisdictional element to defining and accrediting Eligible User Groups, local stakeholders and organizations need to be involved.*
  - *Goal: a result that is credible.*

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

- **Summary of Framework Response**: For private third parties, ICANN would consult with GAC and Eligible User Group members to identify authenticating bodies, which would then develop authentication criteria.
- ***Comment****: Previously, ALAC said "an accreditation program of some sort for access to partial and/or full WHOIS data needs to be developed."*
  - *A true multistakeholder process should be used to develop authentication requirements, rather than merely consulting with GAC.*
- *Previously, ALAC was also "concerned with … the current lack of clarity [on] what … the associated accreditation process will look like and consist of."*
  - *Only slightly more clarity here.*
- *Development process must involve multistakeholder participation, and contemplate multistakeholder oversight and review.*
- *Risk of gaming if Authenticating Body is aligned with "user group,"*
  - *Could become "poacher turned gamekeeper" situation. Challenge is examining gaming possibilities and build mechanisms to avoid them.*

Process Details

4. Who would be required to provide access to non-public WHOIS data?

- **Summary of Framework Response:** Registry operators and registrars would be required to provide access. Some in community have proposed that registrars, but not registry operators, should be required to provide access.
- ***Comment:*** *Both registry operators and registrars must be required to provide access to data under their respective control.*
  - *New gTLDs Whois services are by operated by the registry*
  - *illogical to place the responsibility solely on the registrars regardless of who collects the data.*
  - *Concerns about contractual privity or data subject safeguards should be dealt with contractually.*

5. What would be the overall process for authenticating legitimate users for access [to] non-public WHOIS date under a unified access model?

- **Summary of Framework Response:** Largely leaves the process for authenticating users to the Authenticating Body, other than vaguely suggesting it “could include an application process for example.”
- **Comment:** This raises numerous concerns. Needs much more specificity about who these Authenticating Bodies would be, criteria are for designing Eligible User Groups, information needed for authentication, how authentication will be performed, etc.
- Need oversight and review of these processes, when created and when in operation.
- Need to clarify what constitutes a sufficient “identification” by the accredited user’s legitimate purpose (e.g., whether it needs to contain a “balancing test” analysis).
- Need to clarify role and responsibility of registry or registrar in “evaluating” such identification (e.g., can the registry operator or registrar merely take the accredited user’s statement at face value, or can it conduct its own analysis of the legitimacy of the purpose and the specific request?)

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

- **Summary of Framework Response:** Users get “the level/scope of non-public WHOIS data consistent with the identified legitimate purpose … for each query.” Access on a query-by-query basis; full records would not be returned without legitimate interest in doing so. ICANN will seek guidance from EDPB whether there is a GDPR-compliant model that would allow bulk access and returning full WHOIS data by default.
- ***Comment:*** *Reasonably balanced proposal, though short on specifics.*
- *How will dataset for a particular legitimate purpose be determined? “One size fits all”? A default that can be customized for each query? Whose judgment will be involved?*
- *Bulk access: Many think bulk access breached data protection laws long prior to GDPR. Bulk data and access to bulk data must be more sharply defined. Need an extremely high bar to prove legitimate interest in a wholesale download of the whole, or even part of the database, and that this interest was not outweighed by the rights of the millions of data subjects in that download.*
- *Access to a de-identified stream of selected fields from some subset of the whole (e.g., a particular region or gTLD) e.g., for statistical analysis under controlled circumstances is more likely. “Bulk access by agglomeration” should be prohibited.*
- *If done at all, bulk access must be explicitly and clearly GDPR-compliant .If there is no possible GDPR-compliant method then bulk access cannot be provided*

7. Would registry operators and registrars be required to provide access to non-public WHOIS data to all authenticated users?

- **Summary of Framework Response**: Registries and registrars would be required to provide “global access … consistent with the identified legitimate purpose … subject to applicable local laws.”
- ***Comment****: This seem reasonable, though so vague that it may amount to nothing at all.*

8. Would a unified access model incorporate transparency requirements?

- **Summary of Framework Response:** The Framework contemplates logs of all access requests, unless prohibited by applicable law. Logs would be available to ICANN org for specified purposes, and to data subjects on request (with regard to their own data). Logs will contain personal data of individual users who requested access; rights of these data subjects also need to be protected.
- ***Comment:*** *The ALAC supports appropriate transparency requirements. Data subject rights must be treated in a GDPR-compliant manner – whether registrant or the "Eligible User." However, it may be inappropriate to provide log access (e.g., threat investigations) where the data subject is a malefactor. This requires further consideration.*
- *It is counter to transparency for the Authenticating Body to "maintain, but not publish, a list of authenticated users." They should publish, in a GDPR-compliant fashion, the list of authenticated users.*

9. Would there be any fees as part of a unified access model?

- **Summary of Framework Response:** The Framework does not take a position on this topic.
- ***Comment:*** *From an end-user perspective, it is clearly desirable that no fees be charged, since WHOIS access will often be sought by end-users in varying financial circumstances. Even where an end-user is not the "user," the WHOIS access is likely to benefit end-users directly or indirectly.*

10. Would there be a process to review the effectiveness of a unified access model?

- **Summary of Framework Response:** The UAM would be reviewed at regular intervals.
- ***Comment:*** *The ALAC supports regular review. The Framework does not specify who will conduct the review. The ALAC suggests a combination of multistakeholder reviews and independent third party reviews.*
- *"Self-review" by contracted parties and ICANN org, without further input, would be inappropriate.*

Technical Details

Terms of Use for Accessing Non-Public WHOIS data

11. Would there be a central repository of WHOIS data from which access would be granted to authenticated users?

- **Summary of Framework Response**: Does not contemplate a central repository. It does recognize that some have suggested a central repository or a central portal. These could raise security and legal implications.
- ***Comment***: *It is worthwhile to explore these options in the long run. This would be consistent with the concept of "Thick WHOIS."*
- *These options would require significant study, paradigm shifts, technical development, legal review, security efforts, etc. The advent of IDNs further complicates matters, with different languages and scripts involved.*
- *Any efforts toward a central repository or portal should not delay the implementation of a unified access model.*

12. What technical method would be required to provide access to non-public WHOIS data?

- **Summary of Framework Response:** The Framework states that RDAP would be used.
- ***Comment:*** *This is reasonable and appropriate – and long overdue.*

13. What technical method would be used to authenticate users?

- **Summary of Framework Response**: The Framework calls for “a system of credentials.” Community models have also proposed a system of “credentials, tokens and/or certificates.”
- ***Comment:*** *This is reasonable and appropriate, but lacks details.*
- *Unable to judge whether this will work in practice.*
- *For example, it is unclear whether "credentials, tokens and/or certificates" would have limitations and controls to reduce the risk of unauthorized "transferred" access.*

Terms of Use for Accessing Non-Public WHOIS data

14. What would be the role of Terms of Use in a unified access model?

- **Summary of Framework Response:** Terms of Use would provide a "framework for the use of non-public WHOIS data," notably "appropriate limitations" on use, "proper procedures" for access, and "other safeguards and public policy considerations." "In general, the non-public WHOIS data must be used for the purposes [for which] it was provided, and it must not be forwarded to unauthorized third parties."
- ***Comment:*** *The use of Terms of Use in this context is unexceptional.*
- *Stating that WHOIS data "must be used for the purposes [for which] it was provided" points to a potential "Achilles heel" for any plan for access – it depends a great deal on the purposes specified at the time of collection. Data collected for use in WHOIS needs to be accompanied by an extensive list of the purposes for which WHOIS data will be accessed. The statement that the data must be used "for the purposes it was provided" for appears to goes further than GDPR, which refers in Art. 5(1)(b) to not processing in a manner "incompatible" with the purposes of collection. This requires a neutral legal analysis.*

14. What would be the role of Terms of Use in a unified access model?

- *Framework: WHOIS data "must not forwarded to unauthorized third parties"*
  - *Who is an "unauthorized third party"?*
  - *Narrow view: only the "authenticated user" can receive and view the data. This would be impractical. Access often requires that data be shared with parties who should be considered "authorized" for access to be meaningful.*
- *However, this raises further issues.*
  - *How would the registry operator or registrar know that representative has been appointed?*
  - *Does the registry operator or registrar need to know who the client is?*
  - *How could they be reasonably assured that the representative represents that client (or any client)?*
  - *Will the contracted party, or even the Authenticating Body, be required to verify the "authorized party?*
- *Where data is being accessed for use in a UDRP proceeding, it must be shared with the UDRP provider or the complainant (as the case may be).*
  - *These types of access should be "reasonably expected" and are not "incompatible" with the underlying purpose.*
- *ICANN needs to clarify that those involved in the purpose for which access was sought will be considered "authorized persons."*
- *But personal data should not be retained for future use or to aggregate a database or for any other new purpose.*

15. Would there be multiple Terms of Use?

- **Summary of Framework Response**: Terms of Use would have some common terms and some terms specific to a particular Eligible User Group.
- ***Comment***: *This is reasonable and appropriate – if there is sufficient multistakeholder involvement in and oversight of the drafting process.*
- *Must avoid self-serving terms drafted by and for a particular Eligible User Group (or an allied Authenticating Body.*

16. How would the Terms of Use be developed?

- **Summary of Framework Response**: ICANN org will develop the Terms "in consultation with the GAC and the European Data Protection Board." Each "Authenticating Body" will be responsible for developing "additional safeguards" for the corresponding User Group.
- ***Comment:*** *This proposal is quite remarkable, in that multistakeholder involvement is entirely absent.*
- *Needs to be substantially revised so that there is multistakeholder involvement and oversight.*

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

- **Summary of Framework Response**: Lists a number of categories of safeguards, but is silent about the key issue duration of retention and final deletion of accessed data.
- A number of community suggestions are mentioned, including penalties for abuse/non-compliance with safeguards, an alternative dispute resolution mechanism to allow recourse against users who have abused the access model, and rate limiting of queries for non-public WHOIS data.
- ***Comment****: The ALAC supports these safeguards.*
- *However, safeguards around the timing of retention and deletion should be made explicit.*
  - *One possible option: Make intended data retention period part of data access request*
- *It should be clear that authorized users cannot accumulate data they acquire through their access to WHOIS, e.g., in order to build a shadow database.*
- *Need to clarify what constitutes substantive non-compliance vs. simple error*
- *For true acts of non-compliance, need some form of "teeth", e.g,, suspending access rights.*
- *Do not recommend penalties beyond that, as it isn't clear what constitutes "abuse." It can be a loaded term, used to cast Users in a negative light (as potential "abusers"). Must develop processes for properly identifying the abusing User and for an aggrieved party (or even a "do-gooder") to report such abuse.*

18. What mechanism would be used to require compliance with the Terms of Use?

- **Summary of Framework Response:** The Framework mentions “declaring adherence” to the Terms of Use, and the future possibility of “access agreements.”
- ***Comment:*** *This seems to miss the mark. These are mechanisms to show agreement with the Terms of Use, not methods of requiring compliance with the Terms. However, since this is touched on above and below, we do not need to discuss this item further.*

19. Who would monitor and enforce compliance with Terms of Use?

- **Summary of Framework Response**: Authenticating Bodies would each monitor and enforce compliance with relevant Terms of Use. They would each enter into a "Memorandum of Understanding" with ICANN to ensure appropriate oversight by ICANN. If access model becomes consensus policy or is in contracted party agreements, then ICANN Contractual Compliance would handle compliance issues.
- ***Comment:*** *This raises issues.*
- *Who is the "counterparty" to the User is in the Terms of Use?*
  - *Not likely to be the Authenticating Body, so enforce the Terms seems peculiar at best.*
- *Do the Authenticating Bodies have the resources, expertise or capabilities for monitoring and enforcing compliance?*
- *Contractual Compliance should be involved in contract compliance and enforcement, but should be more of a "watchdog" than it is with current contractual compliance.*
- *If the access model is not part of consensus policy or registry/registrar contracts, then who will provide oversight? Some form of centralized oversight and enforcement (and penalties) is critical to the success of the program. This is a major gap and needs to be further explored.*

Community Views about High-Level Elements of a Unified Access Model

“Competing” Community Views

- Section E identifies areas where ICANN believes there are “competing views.”
- ICANN will weigh the public comments to determine if these differing views can be resolved.
  - It is important for the ALAC to respond to these in a discrete fashion, even if it is somewhat repetitive.

On the “legal requirements of GDPR”

Whether an authenticated user must provide its "legitimate interest" for each individual query.

- **Comment**: Where the "legitimate interest" basis is being relied on, there clearly must be some statement of the "legitimate interest."
- What constitutes a sufficient statement of legitimate interest?
  - A completely generic "cookie-cutter" statement that really says nothing would be insufficient.
  - On the other hand, requiring a detailed and highly customized narrative would be unnecessary and burdensome, and could even be seen as punitive.
- Don't want to see elevated requirements used in an effort to deter appropriate access efforts. A balanced approach is critical.

Whether "full WHOIS data" must be returned in response to the authenticated user's query.

- **Comment**: Expect a "default" set of non-public WHOIS data for each category of access and/or Eligible User Group.
- Beyond the default, additional (including full) non-public WHOIS data should only be returned where that request specifically asks for it and provides a sufficient reason for that additional information.
- On the other hand, default sets should not be so narrow as to restrict utility or require a significant percentage of special requests. Balance is the key.

Whether "full WHOIS data" must be returned in response to the authenticated user's query.

- **Providing access to technical and admin contacts:**
- Where the tech and/or admin contacts are different from the registrant, this data will be particularly useful.
  - This indicates the registrant may not be technically knowledgeable or proficient. As such, contacting the registrant may not be helpful.
  - An issue with the domain may require the efforts of the technical contact and not a registrant without technical expertise or access.
  - There may also be times where there is a hosting issue and the customer of the hosting company is needed to resolve the issue; that customer may be the tech contact and not the registrant.
  - Knowing the admin and tech contacts may provide information that is uniquely helpful in an investigation.

Whether logs of query activities "must" be available to the relevant registrant upon request, unless prohibited by "a relevant court order or legal requirement."

- **Comment**: Registrants should be afforded access to query activity consistent with Art. 15 of the GDPR, which gives the data subject the right to obtain information, including:
  - The "purposes of the processing,"
  - the "categories of personal data concerned"
  - the "recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations."
- Art. 15 requires access to certain data in query logs (e.g., date and time of request, grant of access), but does not require the identity of individual recipients of data to be revealed.
  - It appears sufficient to supply the category of recipients.
  - These rights need to be balanced against other considerations, such as the data subject rights of Users and negative effects of providing access to information that would compromise investigations or threat mitigation efforts, among other things.
  - Users could be given the option of allowing access to the full logs for each query, in the interest of transparency.

On “certain key process elements” of a UAM

Whether registries/registrars must be required to provide access to non-public WHOIS data?

- **Comment**: Registries/registrars must be required to provide access to non-public WHOIS data.
- This is consistent with the intent of the WHOIS services, the intent and implementation of the access model, and a reasonable interpretation of legal obligations.
- In particular, registries and registrars should not seek to thwart or frustrate the purposes of the access model.

Whether there should be a fee for access non-public WHOIS data.

- **Comment:** WHOIS services are an integral part of ICANN's *raison d'etre* and are fundamentally a public service. As such, there are good arguments that it would be inappropriate to charge a fee for access.
- End-users are often the beneficiary, directly or indirectly, of the efforts made possible by WHOIS access.
  - Examples include threat assessment and mitigation, malware defense, "advance fee fraud" enforcement (i.e., requests to send money under various scams, some quite well known almost to the point of cliché), many other anti-fraud efforts, anti-spam efforts, anti-phishing efforts and many other efforts that promote security, stability and trust in the Internet.
- Access model will require additional expense, time and effort on the part of Users, registries, registrars, Authenticating Bodies and ICANN org.
  - It may seem that registrars will bear the brunt of this change.
  - It could be worth exploring what these costs are (for registrars and others) and try to find a method to spread these costs more equitably.
  - Some have suggested that fees might curb "frivolous" requests; however it's difficult to define what would make a request frivolous where a legitimate interest is involved.

Whether there should be a "centralized portal operated by ICANN" where authenticated users can perform queries of non-public WHOIS data.

- **Comment**: A centralized portal needs to be distinguished from a centralized repository, which raises many greater concerns.
- A centralized portal would be very useful and could be used to shift some of the cost and burden away from the registrars.
- On the other hand, it is hardly a requirement that such a portal be put into place. Given the desire for speed and simplicity, it would be hard to justify the development of an additional system – unless the costs were outweighed by the benefits. That is essentially an implementation question, not an ideological or positional question.