At-Large Workspace: ICANN Seeking Community Feedback on Proposed Unified Access Model

Public Comment Close	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
14 November 2018	ICANN Seeking Community Feedback on Proposed Unified Access Model	ADOPTED 14Y, 0N, 0A	Gregory Shatan	06 November 2018	09 November 2018	13 November 2018	16 November 2018	13 November 2018	ICANN GDPR gdpr@icann.org	**AL-ALAC-ST-1118-02-01-EN**

Hide the information below, please click here >>

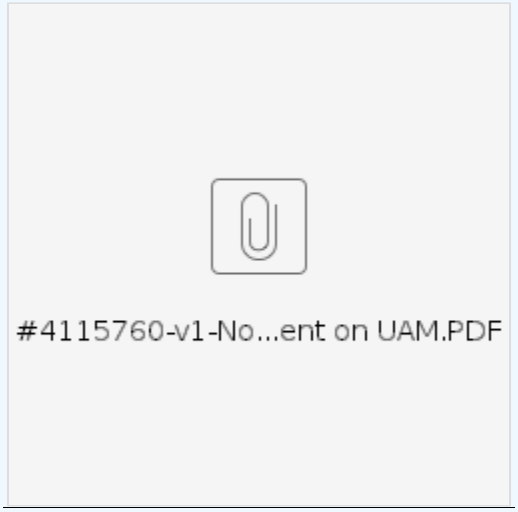
Ratified Version (19 Nov 2018):

AL-ALAC-ST-1118-02-01-EN.pdf

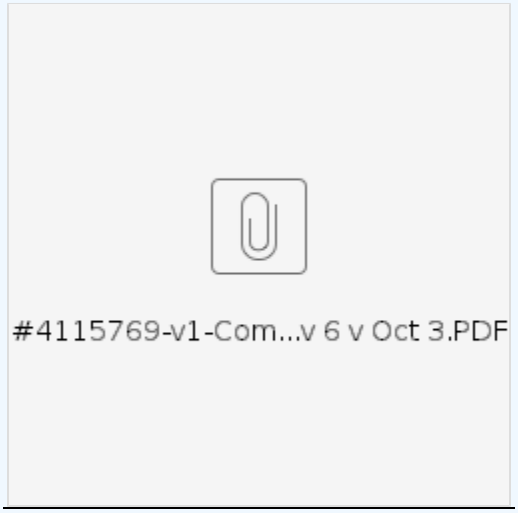
Final Version (13 Nov 2018):

AL-ALAC-ST-1113-01-00-EN.pdf

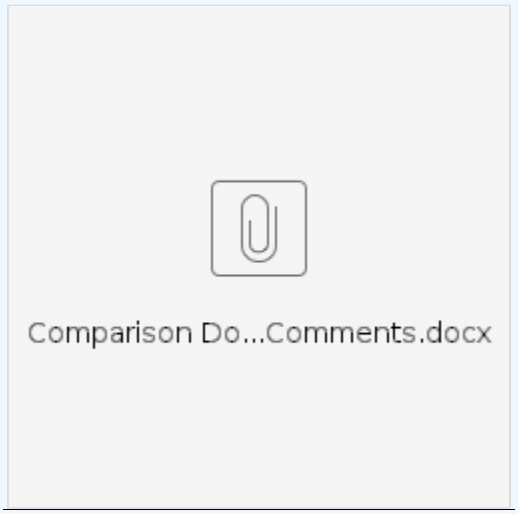
Updated Version (06 Nov 2018):



Comments on Updated Version (06 Nov 2018):



Please see Updated Comments (10 Oct 2018):



Please see updated UAM: https://www.icann.org/en/system/files/files/framework-elements-unified-access-model-for-discussion-20aug18-en.pdf

ICANN 27 July 2018 blog post: Data Protection/Privacy Update: Key GDPR WHOIS Updates and Next Steps

Data Protection/Privacy Update: Additional Guidance from the European Data Protection Board: https://go.icann.org/2mifm4m

Data Protection/Privacy Update: Seeking Community Feedback on Proposed Unified Access Model

Today we're sharing for discussion the draft Framework Elements for a Unified Access Model for Continued Access to Full WHOIS Data [PDF, 93 KB]. At a high-level, it provides a process for how third parties may access non-public WHOIS data.

I also want to take this opportunity to thank the ICANN community for their hard work and valuable inputs that led us to the adoption of the Temporary Specification for gTLD Registration Data (Temp Spec). The European Data Protection Board (EDPB) also recognized these community efforts and said it "expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data." Just as we all worked together to agree on tiered/layered access, which is a major change to the WHOIS services, your contributions here will help us shape this model.

The EDPB also said that it "may engage further with ICANN to ensure that the legal requirements under EU data protection law are properly addressed." We note the importance of community collaboration as we seek this legal certainty. The ICANN Board of Directors, in the Temp Spec, encouraged continued community work "to develop an accreditation and access model that complies with GDPR." To further these community discussions, we have also published a chart [PDF, 90 KB] comparing our draft framework elements against those of two models proposed by ICANN co mmunity members.

The framework lays out a series of central questions to help frame discussions about how such a model may work, including how and which users with a legitimate purpose, as defined by the law, can gain access to non-public registration data. It builds on the "Calzone Model" (Attachment 2), the Temp Spec, and also incorporates ideas from community members and relevant data protection authorities. This proposed unified access model would provide transparency, uniformity, and most importantly foster discussions that may increase legal certainty and simplify the process for all parties.

Because access to non-public registration data is a public policy concern, and public policy is in the purview of governments, ICANN org's proposal is to start by engaging with governments in the European Economic Area, which are also members of the Governmental Advisory Committee (GAC). Some of the questions to be discussed with governments include how law enforcement, individual users and other private third parties would be authenticated to access non-public registration data. There remain open questions on this and other issues for which we welcome your input. For example, the scope of data an eligible user group would have access to may be limited to only the fields a user requires, or the full WHOIS record for a particular query.

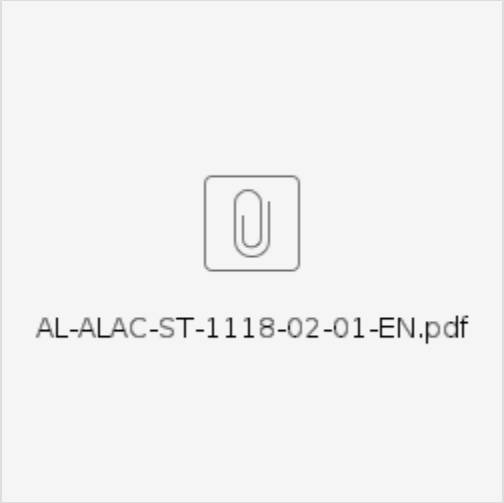
In addition to sharing this framework with the community, we intend to discuss it with the EDPB to ensure the model is compliant with the European Union's General Data Protection Regulation (GDPR).

The community has also raised questions about this draft model and other related activities. I want to note that developing a unified access model has been part of our conversations regarding the GDPR from the start, including an approach outlined in both the Calzone and the Cookbook. Part of ICANN org's role is to facilitate discussions with the data protection authorities (DPAs) to confirm, where possible, that the community's consensus policy is compliant with the GDPR. ICANN continues to maintain a high level of transparency relating to our role. Our community conversations on these issues will help guide our discussions with the DPAs and we will continue to document these discussions.

I encourage you to review the proposed unified access model and participate in community discussions on this topic, including at ICANN62, where there will be several sessions related to the GDPR and the Temp Spec. In addition, you can provide your feedback via email to gdpr@icann.org. Be sure to visit our Data Protection/Privacy page for regular updates and an overview of our activities in this area.

FINAL VERSION SUBMITTED (IF RATIFIED)

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.



FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.

AL-ALAC-ST-1113-01-00-EN.pdf

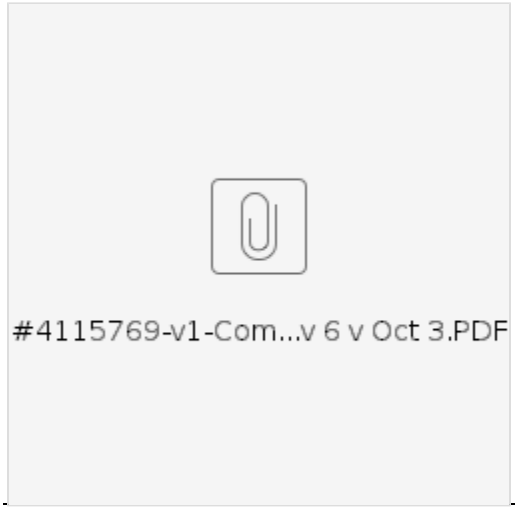
DRAFT SUBMITTED FOR DISCUSSION

The first draft submitted will be placed here before the call for comments begins. The Draft should be preceded by the name of the person submitting the draft and the date/time. If, during the discussion, the draft is revised, the older version(S) should be left in place and the new version along with a header line identifying the drafter and date/time should be placed above the older version(s), separated by a Horizontal Rule (available + Insert More Content control).

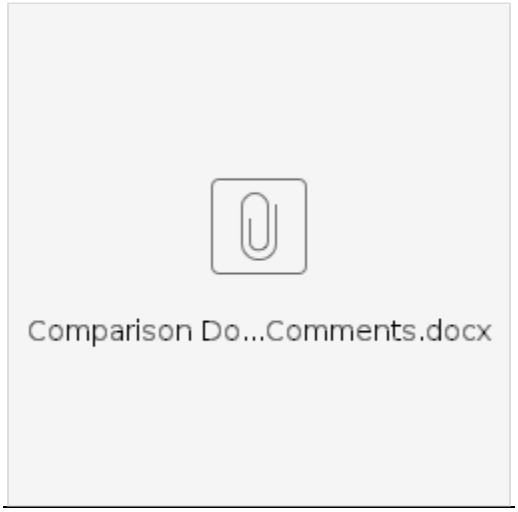
Please see Updated Version (06 Nov 2018):

#4115760-v1-No...ent on UAM.PDF

Please see Comments on Updated Version (06 Nov 2018):



Please see Updated Comments (10 Oct 2018):



Draft by Greg Shatan, 03 October 2018

ALAC Statement on Data Protection/Privacy Issues: Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data

Introduction

The ALAC appreciates the opportunity to provide feedback on the "Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data," published on 20 August.

Prior ALAC Statement regarding Access

On 10 April 2018, the ALAC submitted the "ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model," which includes the following views relating to access to WHOIS. These views are relevant here:

A question to be addressed as part of a layered/tiered approach in the Interim Compliance Model is what data elements can continue to be published in the public layer of WHOIS. And who can then access non-public WHOIS data, and by what method? It seems be 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.

Under the proposed approach, which the ALAC agrees with, user groups with a legitimate interest and who are bound to abide by adequate measures of protection, for example law enforcement agencies and intellectual property lawyers, should be able to access non-public WHOIS data based on explicit pre- defined criteria and limitations under a formal accreditation program. This approach attempts to provide a method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR. Those legitimately combatting cyber abuse including spam, phishing and malware distribution must similarly be given appropriate access, but the methodology for doing so, particularly in the short term is less clear and must urgently be addressed.

As stated, the ALAC is concerned however with regard to the development of the accreditation program, the number of remaining open decision items and the very short timeline before the GDPR is applicable.

The ALAC can only stress the importance of further engagement with EU data protection authorities to define and reach agreement on an accreditation approach that satisfies the requirements of the GDPR, which approach could include the certification of codes of conduct or participation in a data protection certification. As legal analysis and response to community comments indicates.

The ALAC would like to see a reflection from the DPAs on which non-public WHOIS data should be accessible to accredited parties, whether there should be different levels of accreditation (levels of 'layered/tiered access', i.e. to different sets of WHOIS data) and, if so, what the associated criteria should be, and once a party is accredited how access to (a subset of) WHOIS data is provided and if that could be a form of 'bulk' access.

Framework for a Possible Unified Access Model

Before the ALAC responds below to the specific questions and answers offered in the Framework, we offer the following general comments.

First, it goes without saying that this or any "access model" must be compliant with GDPR. Various stakeholders have their views on what constitutes GDPR compliance. While these views should be given due consideration, ICANN org cannot simply rely on them. To varying extents, these may be advocacy pieces rather than neutral analysis, and they may or may not reflect well-informed and well-considered views of GDPR. More fundamentally, they are not legal advice. Therefore, ICANN must seek and receive legal advice from qualified counsel that the model is compliant with GDPR.

Second, the rights and concerns of end-users regarding access to registrant data must always be part of any calculus. WHOIS is the question, and access is the answer. Email recipients should have the right to find out "who is" the person (or thing) sending them e-mail. Website users should have the right to find out "who is" behind the website they are visiting. Mail service providers should have the right to find out "who is" using their resources, and be able to determine if they are spammers. The examples are endless, but unfortunately not often brought up in this process, even though end-users are by far the most numerous participants, and by far the most likely to be harmed by abuse and other violations.

Third, the unified access model must be designed to be scalable and perform at scale. The system cannot depend on manual determinations, when the real world of abuse moves at automated speeds (e.g., "bad guys" registering or compromising thousands of domains per day via automation)). A useful access model should have a well-defined taxonomy of abuse types and other legitimate interest types, domain abuse scenarios, and threat levels. This would feed into a "matrix" that would identify the appropriate information requirements, data to be accessed and response timeframes for that specific type of request. Once there is an agreed-upon set of inputs and outcomes, parties will be able to build or access automated systems to create, accept and respond to WHOIS information requests in an appropriate and consistent fashion.[1]

Fourth, when considering an access model, it's important for the various harms to be balanced in a non-biased fashion, and for the various scenarios to be approached dispassionately and scientifically. Too often, this area becomes an ideological minefield, which in turn tests the multistakeholder model. A more balanced and detached approach is more likely to lead to solid guidance, consistent decision-making and realistic implementation.

Eligibility

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

Summary of Framework Response: The proposed UAM would be open to a "defined set" of "user groups" with "legitimate interests." The Framework describes this as an attempt to strike a balance between types of 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 might request access more rarely. The Framework notes that other elements of the Framework are designed to ensure that data subject rights are adequately protected.

Comment: *The ALAC supports this aspect of the UAM. However, the Framework is very short on specifics and does not define what is meant by "user groups," though it mentions "intellectual property rights holders, law enforcement authorities, operational security researchers, and individual registrants" as examples. Developing this list of "user groups" will be a critical element in the development of the UAM.*

One comment already submitted to ICANN raises the issue of whether third parties should be able to appoint representatives to request and receive access on their behalf (e.g., an investigator or an attorney). This requires further exploration, and consideration of how representatives would be validated or authenticated, and how to be reasonably certain that the representative is bona fide. The Terms of Use (discussed later) could contain terms (e.g., representations and warranties) covering these issues. As a general matter, the access system should not be set up to favor certain user types and disfavor other user types.

2. Who would determine eligibility?

Summary of Framework Response: The Framework proposes that governments within the EEA (and who are GAC members) would identify or "facilitate identification" of broad categories of "Eligible User Groups," after which ICANN org would engage with other governments through GAC to identify specific Eligible User Groups. Examples of such groups include "intellectual property rights holders, law enforcement authorities, operational security researchers, and individual registrants."

Comment: *The ALAC previously commented on a very similar issue in its 10 April 2018 submission, which stated that ALAC "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 relevant to identifying Eligible User Groups or categories of groups, other than governmental users (e.g., law enforcement authorities). Ceding such a vital aspect of the process to governments sets a bad precedent for ICANN as an organization "rooted in the private sector." [2] As we stated in our 10 April Statement, these "should be developed by the entire community, in a true multistakeholder fashion." Of course, governments are stakeholders as well, and their contributions should not be discounted in any way.

As with any multistakeholder process, it is important to keep an eye on the balance between and relative influence of (and even capture by) the various stakeholder sectors. Where there is a geographic or jurisdictional element to defining and accrediting Eligible User Groups, local stakeholders and organizations need to be part of the process. The goal must be a result that is credible.

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

Summary of Framework Response: The Framework states that, for private third parties, ICANN would consult with the GAC and members of the Eligible User Groups to identify bodies with expertise to authenticate users. These Authenticating Bodies would then develop authentication criteria.

Comment: *In its 10 April statement, the ALAC recognized that "an accreditation program of some sort for access to partial and/or full WHOIS data needs to be developed." As noted above and in our 10 April statement, a true multistakeholder process should be used to develop authentication requirements, rather than merely consulting with the GAC.*

In its 10 April statement, the ALAC was also "concerned with regard to the current lack of clarity when it comes to exactly what … the associated accreditation process will look like and consist of." There is more clarity in the current proposal, but only slightly. The ALAC understands the utility and efficiency in using existing accreditation/governing bodies for this purpose – after all, they have already validated members of their user community, albeit for somewhat different purposes. However, the development of the accreditation process must involve multistakeholder participation, and the process itself must be subject to multistakeholder oversight and review.

There are opportunities for gaming in the development and administration of such processes, especially where the Authenticating Body is allied with or part of the "user group." If left unchecked, this could turn into a "poacher turned gamekeeper" situation (not to suggest that any stakeholders can be compared to "poachers," of course). The challenge here is to examine the 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: The Framework states that both registry operators and registrars would be required to provide such access. However, it also notes that some comments from the community have proposed that registrars, but not registry operators, should be required to provide access, and ultimately suggests this would be a "possible" topic for discussion in "any relevant" PDP.

Comment: *The ALAC believes that both registry operators and registrars must be required to provide access to the non-public WHOIS data that is under their respective control. In the new gTLDs, the Whois service is operated by the registry, not the registrars, so it would be illogical to place the responsibility solely on the registrars regardless of who collects the data. Any concerns about contractual privity or data subject safeguards can easily be dealt with contractually. While a future PDP should not be unduly constrained, the Framework should strongly favor, and make the case for, registry and registrar access.*

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: The Framework largely leaves the process for authenticating users to the Authenticating Body, other than vaguely suggesting it "could include an application process for example."

Comment: *Consistent with the ALAC's previous comment above, this raises numerous concerns. There needs to be much more specificity in the proposal about who these Authenticating Bodies would be, what the criteria are for designing Eligible User Groups, what information is needed for authentication, how authentication will be performed, etc.*

Furthermore, there needs to be oversight and review of these processes, both at the time of creation and when in operation. The Framework needs 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). It should also clarify the role and responsibility of the registry operator 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: The Framework states that the users would get "the level/scope of non-public WHOIS data consistent with the identified legitimate purpose … for each query." [NB: Should this be "legitimate interest" rather than "legitimate purpose"?] The document recognizes that there is also support for the view that full WHOIS data for the requested domain name should be returned to the authenticated user. In the end, the Framework takes the position that access to data would be on a query-by-query basis and that full records would not be returned "unless doing so would be supported by the legitimate interest provided by the authenticated user." The report also says that ICANN will seek guidance from the EDPB whether there is a GDPR-compliant model that would allow for bulk access and for returning full WHOIS data by default to authenticated users.

Comment: *Overall, this is a reasonably balanced proposal, though very short (once again) on specifics. How, for example, will the level/scope of non-public WHOIS data for a particular legitimate purpose be determined? Will there be a "one size fits all" approach, or will there be a default that can be customized for each query? Whose judgment will be involved? This leaves a lot to future processes to develop.*

ICANN alludes to one particularly controversial concept – that of "bulk access." There is a commonly held view that bulk access has breached data protection laws long prior to GDPR. However, we need a much sharper definition of what we mean by bulk data and by access to bulk data in order to make a reasoned determination. There would have to be an extremely high bar to prove that any entity has a 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. More likely is, for example, access to a de-identified stream of selected fields from some subset of the whole (e.g., a particular region or gTLD) to be used "in bulk," e.g., for statistical analysis under controlled circumstances (e.g., restricted retention periods, if appropriate). Clearly, "bulk access by agglomeration" should be prohibited (i.e., the building/reconstruction of a bulk database from a multitude of individual queries).

If any type of bulk access is permitted, it needs to be done explicitly and in a clearly GDPR-compliant manner. Conversely, if there is no possible GDPR-compliant method for permitting a given type of bulk access (or any type of bulk access), then bulk access cannot be provided, no matter how useful or attractive it might be to certain Eligible User Groups.

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

Summary of Framework Response: The Framework contemplates that registries and registrars would be required to provide "global access … consistent with the identified legitimate purpose … subject to applicable local laws."

Comment: *Again 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 contemplate some transparency requirements, in particular logs of all access requests, unless logging a request is prohibited by applicable law. These logs would be available to ICANN org for specified purposes, and to data subjects on request (obviously, only with regard to their own data). ICANN notes that the logs will contain personal data of individual users who requested access, and the rights of these data subjects also need to be protected.

Comment: *The ALAC supports appropriate transparency requirements. Certainly, data subject rights must be treated in a GDPR-compliant manner – whether the data subject is the registrant or the "Eligible User." However, there could be instances where it would be inappropriate to provide log access (e.g., threat investigations) where the data subject is a malefactor. This requires further consideration.*

On the other hand, it seems counter to transparency for the Authenticating Body to "maintain, ***but not publish****, a list of authenticated users." The Authenticating Body 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 the concept of regular review. However, the Framework does not specify who will conduct the review, and the Devil is in the details. The ALAC suggests that a combination of multistakeholder reviews and independent third party reviews would be appropriate. On the other hand, "self-review" by contracted parties and ICANN org, without further input, would be inappropriate.*

Technical Details

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

Summary of Framework Response: The Framework does not contemplate a central repository. It does recognize that some commenters have suggested a central repository, or at least a central portal. The document recognizes that these could raise security and legal implications.

Comment: *The ALAC believes that it is worthwhile to explore these options in the long run. The ALAC notes that this would be consistent with the concept of "Thick WHOIS." However, these options would require significant study, paradigm shifts, technical development, legal review, security efforts, etc. The advent of IDNs further complicates matters, with the 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," and notes that community models have also proposed a system of "credentials, tokens and/or certificates."

Comment: *Again, this seems reasonable and appropriate. Again, the devil is in the details, of which there are none. As such, it is premature 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: The document states that 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." The document goes on to state, "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.*

The statement 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 should thus be accompanied by an extensive list of the purposes for which WHOIS data will be accessed. However, the statement -- that the data must be used "for the purposes it was provided" for – appears to goes further than GDPR.[3] This requires a neutral legal analysis.

The statement that WHOIS data "must not forwarded to unauthorized third parties" raises a question that is not answered in this Framework – who is an "unauthorized third party"? This could be narrowly construed so that literally only the "authenticated user" can receive and view the data. This would be an impractical result. Many (if not most) types of access will require that the data be shared with other parties who should be considered "authorized" for access to be meaningful. For example, where an attorney or other designated representative is accessing the data on behalf of a client; the client should be an "authorized party," so the data can be shared with the client.

However, this raises further issues that would need to be resolved. 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 complications arising from identifying the right attorney for the purpose of verifying "authorized party" to a data request?

Similarly, 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." Of course, it should go no further than that; 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: The Framework contemplates Terms of Use that would have some common terms and some terms that are specific to a particular Eligible User Group.

Comment: *This is, again, reasonable and appropriate – as long as there is sufficient multistakeholder involvement in and oversight of the drafting process, to avoid self-serving terms drafted by and for a particular Eligible User Group (or by an Authenticating Body allied with a User Group).*

16. How would the Terms of Use be developed?

Summary of Framework Response: The Framework contemplates development by ICANN org "in consultation with the GAC and the European Data Protection Board," with each "Authenticating Body" responsible for developing "additional safeguards" for the corresponding User Group.

Comment: *This proposal is quite remarkable, in that multistakeholder involvement is entirely absent. This needs to be substantially revised so that there is multistakeholder involvement and oversight. The Terms are the cornerstone of practical and enforceable safeguards.*

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

Summary of Framework Response: The Framework lists a number of categories of safeguards, but the paper is silent about the duration of retention and final deletion of accessed data. The proposal also mentions a number of community suggestions, 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 the safeguards proposed by ICANN org. In addition, safeguards around the timing of retention and deletion should be made explicit. One possible option is to make the intended data retention period part of the data access request, along with a statement of purpose that covers the proposed use of the data and its retention. As noted above, the safeguards should make it clear that the authorized users should not be able to accumulate data that they acquire through their access to Whois, e.g., in order to build a shadow database.*

Non-compliance by Users and by Registries/Registrars is a problem that can reasonably be anticipated, although what constitutes substantive non-compliance, as opposed to simple error, must be clarified. For true acts of non-compliance, some form of "teeth" would be a good idea, such as suspending access rights in whole or in part for a period of time. We would not recommend penalties beyond that. We don't know what, if anything, would constitute "abuse" and thus are wary about discussing it, especially since it is a loaded term that could be intended to cast Users in a negative light (as potential "abusers"). The 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 also mentions 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: The Framework proposes that the Authenticating Bodies would each monitor and enforce compliance with the relevant Terms of Use, and suggests that each Body would enter into a "Memorandum of Understanding" with ICANN to ensure appropriate oversight by ICANN. If the access model becomes part of consensus policy or contracted party agreements, then ICANN Contractual Compliance would handle compliance issues.

Comment: *This raises issues. First it is unclear who the "counterparty" to the User is in the Terms of Use. We don't anticipate that this would be the Authenticating Body, so having that Body enforce the Terms seems peculiar at best. Second, it is unclear whether any of the Authenticating Bodies have any resources, expertise or capabilities related to monitoring and enforcing such compliance. We assume their expertise is in credentialing or membership management. Thus, this does not seem like the correct approach.*

It makes sense to have Contractual Compliance involved in contract compliance and enforcement, as described by the Framework (though we hope that Contractual Compliance will take more of a "watchdog" attitude than it does with current contractual compliance). However, 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

Section E of the Framework document identifies areas where ICANN believes there are "competing views." Since ICANN will be weighing the comments to determine if these view can be resolved, it is important for the ALAC to respond to these in a discrete fashion below, even if it is somewhat repetitive.

<u>On the "legal requirements of GDPR"</u>

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

Comment: *Where "legitimate interest" is being relied on, there clearly must be some statement of the "legitimate interest." The question is what constitutes a sufficient statement of legitimate interest. On the one hand, a completely generic "cookie-cutter" statement that really says nothing would be insufficient. On the other hand, a requirement for a detailed and highly customized narrative would be unnecessary and would burden every stop of the process. It could even be seen as punitive. We would not want to see elevated requirements used in an effort to deter appropriate access efforts. A balanced approach is critical.*

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

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

We note that a good deal of attention has been paid to the issue of providing access to technical and admin contacts. Where the tech and/or admin contacts are different from the registrant, this hints at good reasons why this data will be particularly useful. As a general matter, this is an indicator that 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.

1. 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 from the controller access to certain information, including the "purposes of the processing," the "categories of personal data concerned" and 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." While Art. 15 requires access to certain data in the logs of query activities, such as the date and time of the request or the grant of access, it does not require that the identity of the individual recipients of data be revealed. It appears sufficient to supply the category of recipients. Furthermore, these rights need to be balanced against other considerations, such as the data subject rights of Users and the negative effects of providing access to information that would compromise investigations or threat mitigation efforts, among other things. That said, Users could be given the option of allowing access to the full logs for each query, in the interest of transparency.*

<u>On "certain key process elements" of a UAM</u>

1. Whether registries/registrars must be required to provide access to non-public WHOIS data;

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

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

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, such as 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.*

Of course, the 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.

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

Comment: *A centralized <u>portal</u> needs to be distinguished from a centralized <u>repository</u>, 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.*

The ALAC appreciates the opportunity to provide these comments and looks forward to further development of the Unified Access Model. WHOIS was designed and meant to be used through some form of access. Without access, WHOIS is essentially useless and meaningless. However, unfettered and uncontrolled access is clearly a problem under GDPR. We applaud the efforts undertaken by ICANN to attempt to create a realistic access model.

[1] For example, a wide-scale, current phishing attack using a compromised website merits providing the requestor very timely access (i.e., within minutes) to the technical and registrant contact data (primarily e-mail and phone number), both to facilitate solving the phishing attack and to mitigate the potential that the victimized registrant's compromised website or domain could be used to expose PII of the registrant or users of the registrant's website.

In contrast, response time relating to a potentially malicious set of domain registrations highly likely to be used in various fraudulent and illegal scams could be somewhat longer (e.g., a day), but would require full information about the registrant and if possible other domains registered around the same time.

In the first instance, registrant access to query logs would not be an issue (because the registrant is a victim); in the second case, registrant access to query logs would be highly detrimental and should require a process to determine if such access can be granted.

[2] ICANN Bylaws, Section 1.2(b)(vi).

[3] *GDPR Art. 5(1)(b) states that personal data should "not [be] further processed in a manner that is incompatible with" the purposes of collection. Similarly, Recital 47 states "whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place" is an important aspect of a "legitimate interest" analysis. Thus, the list of purposes for collection must embrace the legitimate purposes for access, but need not be exhaustive. The proper test is whether a purpose for access is "not incompatible" with the purposes stated at the time of collection and could have been "reasonably expected" by the data subject at the time of collection. This is not hugely different, but it points to a degree of flexibility in the GDPR that is absent in the Framework statement.*

Draft by Greg Shatan, 12 Sep 2018

ALAC Statement on Data Protection/Privacy Issues: Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data

Introduction

As part of ICANN's continuing efforts to address the impact of the European Union's General Data Protection Regulation (GDPR) on the collection, retention and display of registration data in WHOIS services, ICANN published on 20 August 2018, the "Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data." This follows on ICANN's earlier (and shorter) "Framework Elements for Unified Access Model," published 18 June 2018. The ALAC appreciates the opportunity to provide feedback on the proposed Framework for a Possible Unified Access Model (UAM).

The ICANN CEO stated in an accompanying blog post:

"[The community's] feedback will be important as we continue our dialogue with the European Data Protection Board (EDPB) in order to seek legal clarity for any such access mechanism. Lowering the legal risks for data controllers/contracted parties is necessary to develop a workable unified access model."

As noted in the blog post, ICANN is responding in part to the May 27 statement by the European Data Protection Board (EDPB), which said:

"As expressed also in earlier correspondence with ICANN (including this letter of December 2017 and this letter of April 2018), WP29 expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data."

The Proposed Framework for a Unified Access Model

In this iteration, ICANN has proposed "a working draft framework for a possible unified approach to allow continued access to full WHOIS data for authenticated users with a legitimate interest for accessing non-public WHOIS data consistent with" GDPR.

The Framework contemplates a system where a third party that is part of an "eligible user group" could apply for and receive credentials from an "accrediting body" (also referred to as an "authenticating body"). Once accredited, the user would agree to Terms of Use, which would include provisions designed to adequately safeguard personal data that may be made available to the accredited user. When an accredited user wants to get access to WHOIS information, the user would submit a query to the relevant registry operator or registrar through an RDAP service. The query submission would require the user to specify its purpose for accessing the data, and could also require the user to agree to additional terms of the registry/registrar. The registry/registrar would then "validate" the credentials with the relevant authenticating body. After validation, the registry/registrar would provide user access to the non-public WHOIS data elements "consistent with the legitimate purpose identified in the query."

In Section E of the Framework document (Community Views about High-Level Elements of a Unified Access Model) ICANN identifies three elements where it believes there is "convergence." ICANN also identifies six areas where ICANN believes there are "competing views," regarding either "legal requirements of GDPR" or "certain key process elements" of a UAM. These will be addressed below.

Prior ALAC Statements Regarding Access

On 10 April 2018, the ALAC submitted the "ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model." This Statement included the following views relating to access:

A question to be addressed as part of a layered/tiered approach in the Interim Compliance Model is what data elements can continue to be published in the public layer of WHOIS. And who can then access non-public WHOIS data, and by what method? It seems be 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.

Under the proposed approach, which the ALAC agrees with, user groups with a legitimate interest and who are bound to abide by adequate measures of protection, for example law enforcement agencies and intellectual property lawyers, should be able to access non-public WHOIS data based on explicit pre- defined criteria and limitations under a formal accreditation program. This approach attempts to provide a method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR. Those legitimately combatting cyber abuse including spam, phishing and malware distribution must similarly be given appropriate access, but the methodology for doing so, particularly in the short term is less clear and must urgently be addressed.

As stated, the ALAC is concerned however with regard to the development of the accreditation program, the number of remaining open decision items and the very short timeline before the GDPR is applicable.

The ALAC can only stress the importance of further engagement with EU data protection authorities to define and reach agreement on an accreditation approach that satisfies the requirements of the GDPR, which approach could include the certification of codes of conduct or participation in a data protection certification. As legal analysis and response to community comments indicates.

The ALAC would like to see a reflection from the DPAs on which non-public WHOIS data should be accessible to accredited parties, whether there should be different levels of accreditation (levels of 'layered/tiered access', i.e. to different sets of WHOIS data) and, if so, what the associated criteria should be, and once a party is accredited how access to (a subset of) WHOIS data is provided and if that could be a form of 'bulk' access.

Framework for a Possible Unified Access Model

The document describes the UAM through a series of questions and answers, broken down into categories. Most of the proposed Framework seems to be quite reasonable. The ALAC's views on each of these specific topics is stated below.

On a more general level, it is critical that the unified access model be scalable and perform at scale. A system that is dependent on manual determination of issues by all parties will not be useful in the real world of abuse that moves at automated speeds (e.g., bad guys registering or compromising domains at scale (each using thousands of domains per day via automation)). A useful access model should have a well-defined taxonomy of abuse types and other legitimate interest types, domain abuse scenarios (e.g. abusively registered, compromised in-part, compromised in-full), and threat level (e.g. ongoing mass attack, ongoing targeted attack, potential attack). This information would support a coordinated understanding (e.g., a matrix) of the information required, the information about Users that can be readily revealed, the actions to be taken and the necessary timeframes. For example, where there is a wide-scale, current phishing attack using a compromised website, very timely access (i.e., within minutes) to the technical contact and registrant contact data (primarily e-mail and phone number) would facilitate solving both the phishing attack and the potential for the registrant to be exposing PII of its own users given that their website tied to a domain is compromised. In contrast, detection of a potentially malicious set of domain registrations highly likely to be used to launch various fraudulent and illegal scams based on prior observed behavior could tolerate a somewhat longer-term response (e.g., a day), but would require full information about the registrant and if possible other domains registered around the same time. In the first instance, access to query logs by the registrant would not be an issue (because the registrant is a victim); in the second case, registrant access to query logs would be highly detrimental and should require a process to determine if such access can be granted. Once there is a common understanding, parties will be able to build or access automated systems to create and accept responses for contact information requests.

It's important for the various harms to be balanced in a non-biased fashion, and for the various scenarios to be approached dispassionately and scientifically. Too often, this area becomes an ideological minefield, which in turn tests the multistakeholder model. A more balanced and detached approach is more likely to lead to solid guidance, decision-making and implementation.

We should also keep in mind the rights of end users in all of this. Doesn't an email recipient have the right to know the true identity of the person (or thing) sending them e-mail? Doesn't a mail service provider have the right to know who is using their resources and determine if they are a spammer? The examples are endless, but unfortunately not often brought up in this process, even though end users are by far the most numerous participants, and by far the most likely to be harmed by abuse and other violations.

Eligibility

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

The proposed UAM would be open to a "defined set" of "user groups" with "legitimate interests." The Framework describes this as an attempt to strike a balance between types of 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 might request access more rarely. The Framework notes that other elements of the Framework are designed to ensure that data subject rights are adequately protected.

It seems self-evident that a UAM would need to be based on a finite list of types of third parties likely to have legitimate interests in accessing non-public WHOIS data. This list should not be exhaustive, and needs to be fairly limited – not to exclude third parties with legitimate interests from access (since they will not be excluded), but rather to give this process the best chance of being completed in a realistic timeframe. The Framework is very short on specifics and does not define what is meant by "user groups," though it mentions "law enforcement authorities" and "intellectual property rightsholders." Clearly, these are just examples. Developing this list of "user groups" will be a critical element in the development of the UAM. While it is premature to focus on any single potential user group, one submission suggests that IP rightsholder access should be limited to the "individual rightsholder" of a "specific IPR" and should not include "any agent or other third party" (e.g., attorneys, brand protection firms, etc.). This has no benefit to end users; rather, it would be detrimental, since end users (as both Internet users and as consumers) often benefit from many forms IP rights enforcement. It is also unworkable, and unfairly restricts the rights of people and entities to seek representation. The ALAC does not support this suggestion.

2. Who would determine eligibility?

The Framework proposes that governments within the EEA (and who are GAC members) would identify or "facilitate identification" of broad categories of "Eligible User Groups," after which ICANN org would engage with other governments through GAC to identify specific Eligible User Groups. Examples of such groups include "intellectual property rights holders, law enforcement authorities, operational security researchers, and individual registrants."

The ALAC previously commented on a very similar issue in the "ALAC Statement on Data Protection/Privacy Issues: ICANN Proposed Interim Model," submitted 10 April 2018, which stated that ALAC "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."

Consistent with these earlier views, ALAC doubts that governments via the GAC should be given such a prominent role in developing the Eligible User Groups. Rather, these Eligible User Groups "should be developed by the entire community, in a true multistakeholder fashion." We expect that most Eligible User Groups will be non-governmental in nature (just as three of the four examples are non-governmental). Governments do not possess any special knowledge, experience or authority relevant to identifying Eligible User Groups or categories of groups, other than governmental users (e.g., law enforcement authorities). Subcontracting such a vital aspect of the process to governments sets a bad precedent for ICANN as a "private sector led organization" and may even be inconsistent with the ICANN Bylaws.

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

The Framework states that, for private third parties, ICANN would consult with the GAC and members of the Eligible User Groups to identify bodies with expertise to authenticate users. These Authenticating Bodies would then develop authentication criteria.

In its 10 April 2018 statement, the ALAC recognized that "an accreditation program of some sort for access to partial and/or full WHOIS data needs to be developed." However, ALAC remains concerned with the prominent role of governments generally and the GAC specifically, and the exclusion of other stakeholders (aside from those being "authenticated") in the identification of potential Authenticating Bodies. Governments do not necessarily have particular expertise with regard to accrediting bodies, many of which are likely to be private sector organizations (e.g., NGOs and trade associations). This should be done in a true multistakeholder fashion, with participants from a variety of stakeholder groups...

In its 10 April 2018 statement, the ALAC was also "concerned with regard to the current lack of clarity when it comes to exactly what … the associated accreditation process will look like and consist of." There is more clarity in the current proposal, but only slightly. The ALAC understands the utility and efficiency in using existing accreditation/governing bodies for this purpose – after all, they have already validated members of their user community, albeit for somewhat different purposes. However, the development of the accreditation process must involve multistakeholder participation, and the process itself must be subject to multistakeholder oversight and review. There are opportunities for gaming in the development and administration of such processes, especially where the Authenticating Body is allied with or part of the "user group." If left unchecked, this could turn into a "poacher turned gamekeeper" situation (not to suggest that any stakeholders can be compared to "poachers," of course). The challenge here is to examine the gaming possibilities and build mechanisms to avoid them.

Process Details

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

The Framework states that both registry operators and registrars would be required to provide such access. However, it also notes that some comments from the community have proposed that registrars, but not registry operators, should be required to provide access, and ultimately suggests this would be a "possible" topic for discussion in "any relevant" PDP.

The ALAC believes that both registry operators and registrars must be required to provide access. In the new gTLDs, the WHOIS service is operated by the registry, not the registrars, so it would be illogical to place the responsibility on the registrars. Any concerns about contractual privity or data subject safeguards can easily be dealt with contractually. While a future PDP should not be unduly constrained, the Framework should strongly favor, and make the case for, registry and registrar access.

As further support for this, some have noted that the boundary between the two business categories has become blurred since the flawed vertical integration practice was allowed.

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

The Framework largely leaves the process for authenticating users to the Authenticating Body, other than vaguely suggesting it "could include an application process for example."

Consistent with the ALAC's comment above, there needs to be oversight and review of these processes, both at the time of creation and when in operation.

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

The Framework states that the users would get "the level/scope of non-public WHOIS data consistent with the identified legitimate purpose … for each query." (Should this say "legitimate interest" rather than "legitimate purpose"?) The document recognizes that there is also support for the view that full WHOIS data for the requested domain name should be returned to the authenticated user. In the end, the Framework takes the position that access to data would be on a query-by-query basis and that full records would not be returned "unless doing so would be supported by the legitimate interest provided by the authenticated user." The report also says that ICANN will seek guidance from the EDPB whether there is a GDPR-compliant model that would allow for bulk access and for returning full WHOIS data by default to authenticated users.

Overall, this is a reasonably balanced proposal, though very short on specifics. How, for example, will the level/scope of non-public WHOIS data for a particular legitimate purpose be determined? Will there be a "one size fits all" approach, or will there be a default that can be customized for each query? Whose judgment will be involved? This leaves a lot to future processes to develop...

ICANN alludes to one particularly controversial concept – that of "bulk access." There is a commonly held view that bulk access has breached data protection laws long prior to GDPR. However, we need a much sharper definition of what we mean by bulk data and by access to bulk data. There would have to be an extremely high bar to prove that any entity has a 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. More likely is, for example, access to a stream of selected fields from some subset of the whole (e.g., a particular region or gTLD) to be used "in bulk," e.g., for statistical analysis under controlled circumstances (e.g., restricted retention periods, if appropriate). "Bulk access by agglomeration" should be prohibited (i.e., the building of a bulk database from a multitude of individual queries). If any type of bulk access is permitted, it needs to be done explicitly.

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

The Framework contemplates that registries and registrars would be required to provide "global access … consistent with the identified legitimate purpose … subject to applicable local laws."

Again this seem reasonable, though so vague that it may amount to nothing at all.

8. Would a unified access model incorporate transparency requirements?

The Framework does contemplate transparency requirements, in particular logs of all access requests, unless logging a request is prohibited by applicable law. These logs would be available to ICANN org for specified purposes, and to data subjects on request (obviously, only with regard to their own data). ICANN notes that the logs will contain personal data of individual users who requested access, and the rights of these data subjects also need to be protected.

The ALAC supports appropriate transparency requirements. It goes without saying that data subject rights must be treated in a GDPR-compliant manner. However, there could be instances where it would be inappropriate to provide log access (e.g., threat investigations) where the data subject is a malefactor. This requires further consideration.

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

The Framework does not take a position; rather, it lists options that have been suggested by comments from various parts of the community. These include fees to Authenticating Bodies, as well as fees paid to registries and registrars in exchange for access. Other comments stated that no fees should be charged, since WHOIS is a critical resource provided in the public interest.

From an end user perspective, it is clearly desirable that no fees be charged, since WHOIS access will often be sought by end users. 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?

The UAM would be reviewed at regular intervals.

The ALAC supports the concept of regular review. However, the Framework does not specify who will conduct the review, and the devil is in the details. The ALAC suggests that a combination of multistakeholder reviews and independent third party reviews would be appropriate. On the other hand, "self-review" by contracted parties and ICANN org, without further input, would not be.

Technical Details

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

The Framework does not contemplate a central repository. It does recognize that some commenters have suggested a central repository, or at least a central portal. The document recognizes that these could raise security and legal implications.

The ALAC believes that it is worthwhile to explore these options in the long run. The ALAC notes that this would be consistent with the concept of "Thick WHOIS." However, these options would require significant study, paradigm shifts, technical development, legal review, security efforts, etc. The advent of IDNs further complicates matters, with the 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?

The Framework states that RDAP would be used.

This is reasonable and appropriate – and long overdue.

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

The Framework calls for "a system of credentials," and notes that community models have also proposed a system of "credentials, tokens and/or certificates."

Again, this seems reasonable and appropriate. Of course, the devil is in the details, of which there are none. As such, it is premature to judge whether this will work in practice.

Terms of Use for Accessing Non-Public WHOIS data

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

The document states that 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." The document goes on to state, "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.

The use of Terms of Use in this context is unexceptional.

The statement 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 should thus be accompanied by an extensive list of the purposes for which WHOIS data will be accessed. However, the statement -- that the data must be used "for the purposes it was provided" for -- goes further than GDPR. GDPR Art. 5(1)(b) states that personal data should "not [be] further processed in a manner that is incompatible with" the purposes of collection." Similarly, Recital 47 states "whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place" is an important aspect of a "legitimate interest" analysis. Thus, the list of purposes for collection must embrace the legitimate purposes for access, but need not be exhaustive. The proper test is whether a purpose for access is "not incompatible" with the purposes stated at the time of collection and could have been "reasonably expected" by the data subject at the time of collection. This is not hugely different, but it points to a degree of flexibility in the GDPR that is absent in the Framework statement.

The statement that WHOIS data "must not forwarded to unauthorized third parties" raises a question that is not answered in this Framework – who is an "unauthorized third party"? This could be narrowly construed so that literally only the "authenticated user" can receive and view the data. This would be an absurd result. Many (if not most) types of access will require that the data be shared with other parties who should be considered "authorized" for access to be meaningful. For example, an attorney may be accessing the data on behalf of a client; the client must be considered an "authorized party." Similarly, where data is being accessed for use in a UDRP proceeding, it must be shared with the UDRP provider. 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." Of course, it should go no further than that; 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?

The Framework contemplates Terms of Use that would have some common terms and some terms that are specific to a particular Eligible User Group.

This is, again, reasonable and appropriate – as long as there is sufficient multistakeholder involvement in and oversight of the drafting process, to avoid self-serving terms drafted by and for a particular Eligible User Group (or by an Authenticating Body allied with a User Group).

16. How would the Terms of Use be developed?

The Framework contemplates development by ICANN org "in consultation with the GAC and the European Data Protection Board," with each "Authenticating Body" responsible for developing "additional safeguards" for the corresponding User Group.

This proposal is quite remarkable, in that multistakeholder involvement is entirely absent. This needs to be substantially revised so that there is multistakeholder involvement and oversight. The Terms are the cornerstone of practical and enforceable safeguards.

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

The Framework lists a number of categories of safeguards, but the paper is silent about the duration of retention and final deletion of accessed data. The proposal also mentions a number of community suggestions, 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.

The ALAC supports the safeguards proposed by ICANN org. In addition, safeguards around the timing of retention and deletion should be made explicit. One possible option is to make the intended data retention period part of the data access request, along with a statement of purpose that covers the proposed use of the data and its retention. As noted above, the safeguards should make it clear that the authorized users should not be able to accumulate data that they acquire through their access to WHOIS, e.g., in order to build a shadow database.

Non-compliance by Users and by Registries/Registrars is a problem that can reasonably be anticipated, although what constitutes substantive non-compliance, as opposed to simple error, must be clarified. For true acts of non-compliance, some form of "teeth" would be a good idea, such as suspending access rights in whole or in part for a period of time. We would not recommend penalties beyond that. We don't know what, if anything, would constitute "abuse" and thus are wary about discussing it, especially since it is a loaded term that could be intended to cast Users in a negative light (as potential "abusers").

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

The Framework mentions "declaring adherence" to the Terms of Use, and also mentions the future possibility of "access agreements."

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 so need to discuss this item further.

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

The Framework proposes that the Authenticating Bodies would each monitor and enforce compliance with the relevant Terms of Use, and suggests that each Body would enter into a "Memorandum of Understanding" with ICANN to ensure appropriate oversight by ICANN. If the access model becomes part of consensus policy or contracted party agreements, then ICANN Contractual Compliance would handle compliance issues.

This raises issues. First it is unclear who the "counterparty" to the User is in the Terms of Use. We don't anticipate that this would be the Authenticating Body, so having that Body enforce the Terms seems peculiar at best. Second, it is unclear whether any of the Authenticating Bodies have any resources, expertise or capabilities related to monitoring and enforcing such compliance. We assume their expertise is in credentialing or membership management. Thus, this does not seem like the correct approach.

It makes sense to have Contractual Compliance involved in contract compliance and enforcement, as described by the Framework (though we hope that Contractual Compliance will take more of a "watchdog" attitude than it does with current contractual compliance). However, 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 an unforgivable gap and needs to be further explored.

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

Section E of the Framework document identifies several elements where ICANN believes there is "convergence":

- Using RDAP;
- Implementing strong safeguards to prevent and combat abuse of non-public WHOIS data provided to authenticated users; and
- Using a "decentralized" process for developing authentication criteria and methods, by using existing entities with "relevant expertise" to authenticate users from particular user groups.

The ALAC concurs with each of these elements of convergence. Some have suggested that, if decentralization is done on a geographical basis, there should be no extraterritoriality, notably with law-enforcement. However, where there are multijurisdictional (or even global) Authenticating Bodies, there is no reason to exclude them out of hand, particularly if their competency has already been recognized in multiple jurisdictions. In any event, it does not appear that decentralization is intended to take place along geographic lines.

The document also identifies areas where ICANN believes there are "competing views":

On the “legal requirements of GDPR”

1. Whether an authenticated user must provide its “legitimate interest” for each individual query;

Where “legitimate interest” is being relied on, there clearly must be some statement of the “legitimate interest.” The question is what constitutes a sufficient statement of legitimate interest. On the one hand, a completely generic “cookie-cutter” statement that really says nothing would be insufficient. On the other hand, a requirement for a detailed and highly customized narrative would be unnecessary and would burden every stop of the process. It could even be seen as punitive. We would not want to see elevated requirements used in an effort to deter appropriate access efforts. A balanced approach is critical...

2. Whether "full WHOIS data” must be returned in response to the authenticated user’s query; and

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

We note that a good deal of attention has been paid to the issue of providing access to technical and admin contacts. Where the tech and/or admin contacts are different from the registrant, this hints at good reasons why this data will be particularly useful. As a general matter, this is an indicator that 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.

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

Registrants should be afforded access to query activity consistent with Art. 15 of the GDPR, which gives the data subject the right to obtain from the controller access to certain information, including the “purposes of the processing,” the “categories of personal data concerned” and 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.” While Art. 15 requires access to certain data in the logs of query activities, such as the date and time of the request or the grant of access. It also does not require that the identity of the individual recipients of data; it is sufficient to supply the category of recipients. Furthermore, these rights need to be balanced against other considerations, such as the data subject rights of Users and the negative effects of providing access to information that would compromise investigations or threat mitigation efforts, among other things. That said, 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

4. Whether registries/registrars must be required to provide access to non-public WHOIS data;

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

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

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, such as 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.

Of course, the 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.

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

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.

The ALAC appreciates the opportunity to provide these comments and looks forward to further development of the Unified Access Model. WHOIS was designed and meant to be used through some form of access. Without access, WHOIS is essentially useless and meaningless. We applaud the efforts of ICANN to create a realistic access model.