ICANN | GAC

Governmental Advisory Committee

Distribution	Public
Date	16 October 2018

The Governmental Advisory Committee's Initial Comments on the Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data

ICANN's Governmental Advisory Committee (GAC) appreciates the ICANN organization's 20 August 2018 Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data ("Draft Framework") that is intended to further discussions about such a Unified Access Model (UAM).

The GAC also welcomes ICANN's recognition that the European Data Protection Board (EDPB) (formerly the Article 29 Working Group), the European Commission, and the GAC all support the development of a unified access model.

The GAC believes that ICANN and the community should strive to develop a comprehensive, harmonized, reliable, and scalable model that allows access to non-public WHOIS data for authenticated users with a legitimate purpose in a manner that is consistent with the EU's General Data Protection Regulation (GDPR).

The GAC considers the development and implementation of such a unified and reliable access model to be of the utmost importance. Existing requirements in the Temporary Specification for contracted parties to provide "reasonable access" to non-public information are insufficient and at best, encourage a fragmented system potentially consisting of thousands of distinct procedures and policies depending upon the registrar involved. The public policy aspects of the Domain Name System (DNS) cannot rely on the individualized policies of 2,500 gTLD registrars and registries. Furthermore, while the GAC appreciates the reference to the GAC's Panama Communique that highlights the "negative impact that the lack of timely access to non-public WHOIS data is having" the GAC urges ICANN to set forth a specific timeline for adopting and implementing the UAM.

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

Regarding the Community's views about high-level elements of a UAM (Draft Framework at 7-8), the GAC supports:

- Using a Registration Data Access Protocol (RDAP) as a technical method for accessing data
- Strong safeguards to guide access to WHOIS data in order to prevent and deter abuse or misuse of WHOIS data
- Decentralized authentication methods/bodies for each type of legitimate user of WHOIS data, including law enforcement authorities and other public enforcement authorities (e.g. consumer protection and public safety agencies); Cybersecurity organisations; and intellectual property rights holders.

The GAC expresses the following views on the Community's "competing views on the legal requirements of the GDPR as they relate to a unified access model" (*Id.* at 7):

1. While the GAC recognizes the need for authenticated users to show a legitimate interest or other legal basis under the GDPR in order to access WHOIS data, the GAC believes that the specifics of how authenticated users demonstrate the requirements of the applicable legal basis should depend on the user group. Law enforcement, for example, would likely operate on the same legal basis (e.g. public interest) for each query of the WHOIS data. In addition, law enforcement often needs to be able to conduct multiple queries at once, for example to combat large botnets. Requiring law enforcement users to specify the legal basis for each individual query would create a burden. Instead, possible alternatives should be considered, such as asking law enforcement users to identify the legal basis for each session[1], as a more efficient method which would allow law enforcement to continue to protect individual users in cyberspace at the pace demanded by the growth and use of the internet.[2]

2. The GAC believes that providing logs of query activities to registrants has the potential to compromise law enforcement and national security investigations. Such a compromise could result in the target of the investigation fleeing the jurisdiction, destroying evidence, and possibly even harming potential witnesses. Therefore appropriate safeguards need to be incorporated in the system, with a view to protect the confidentiality of investigations.

[1] A session is understood to consist of a sequence of WHOIS queries made by a single end-user during the span of a single connection to a WHOIS database or an access portal. A session may consist of a series of queries with a consistent underlying user need.

[2] Other users of WHOIS data might also potentially benefit from the ability of conducting multiple queries at once in order, for example, to assess whether a pattern of bad faith infringements existed.

3. The GAC believes that both registry and registrar operators should be required to provide access to non-public registration data to the greatest extent possible in accordance with the applicable legal basis.

4. The GAC would have concerns about assigning fees and creating unnecessary barriers to entities that may have limited resources. Many entities with important public policy and public safety mandates have small budgets and costs could deter or prevent them from accessing information necessary to protect the public interest.

5. The GAC would support a single user interface provided by ICANN that would allow users to perform queries of non-public WHOIS data on the basis of an authentication provided by ICANN. Such an interface could be easier to implement, minimize confusion among authenticated users, and provide reassurances to the contracted parties. The GAC would be encouraged to see ICANN take on this role, which is consistent with ICANN's role as a (joint) data controller of WHOIS data as articulated in its bylaws. We also note that ICANN is particularly well placed to assume this role because it is the only joint controller of the whole data set (each contracting party only being a joint controller for the subset on their portfolio of DNs).

   While the GAC sees value in ICANN providing an interface allowing authenticated users to perform queries of non-public WHOIS data, more details need to be provided on whether ICANN's role would only consist of validating third parties and their requests or also of actually transmitting the data from the relevant databases maintained by the registries and the registrars. In the latter case, an in-depth analysis of the data flows would be required to better assess the feasibility of this option under the GDPR. The GAC would appreciate more information on evaluation of these options and their positive and negative implications for interested parties.

   The GAC also encourages ICANN to continue exploring all possible methods for ICANN to be acknowledged as the "coordinating authority of the WHOIS system" given its role as a controller (*Id.* at 6) and would appreciate more information on what steps ICANN could take.

Eligibility (Questions 1-3)

Regarding eligibility issues under the Summary Description of a Framework for a Possible Unified Access Model (*Id.* at 8-10), the GAC supports the approach of identifying relevant "user groups" or categories, because different needs and legal requirements should be considered and recognized for the different types of users seeking access to the redacted WHOIS data[3].

The GAC believes that in addition to defined user groups, the UAM should contain procedures for the public at large because they too may have legitimate interests in seeking data.

The GAC believes that all governments represented in the GAC should be involved in identifying eligible user groups at the same time. Potential harms that arise from lack of access to nonpublic WHOIS data is risk for countries both within and outside of the EU.

A UAM must be built with sufficient accountability and liability where appropriate. However, the issues surrounding accountability and liability are complex and require careful assessment and balancing. The GAC encourages further reflection on the role and tasks of authenticating bodies, criteria for selection of authenticating bodies, redress and complaint mechanisms, as all these aspects are not being addressed in the UAM. It is also important to ensure that, within any authenticating body, no conflicts of interest arise between their current mandate and their role as an authenticating body and that appropriate consideration is given to the specific tasks, required technical infrastructure and resources that the authenticating bodies will have to provide. In addition, authentication bodies should not be unfairly made an exclusive provider of these services.

Finally, the GAC believes that a decentralized model for determining authentication requirements for a specific user group makes sense. However, ICANN should provide clear guidance to the authenticating bodies. And such authenticating bodies should be part of a timely ICANN-led process to establish such guidance.

[3] For instance, intellectual property rights holders may have a legitimate interest in getting access to non-public WHOIS data, notably enforcing their rights against illegal website content or bad faith domain registration.

Process Details (Questions 4-10)

Regarding process details under the Summary Description of a Framework for a Possible Unified Access Model (*Id.* at 10-13), the GAC supports both registry and registrar operators being required to provide access within the UAM.

As mentioned above, while the GAC recognizes the need to show a legitimate interest or other legal basis under the GDPR when accessing WHOIS data, the GAC believes that the specifics of how the requirements of the applicable legal basis are demonstrated should depend on the user group. In particular, law enforcement agents often have a legitimate need to conduct multiple queries, such as when identifying or mitigating a large-scale botnet threat. Therefore, requiring law enforcement users to specify a legal basis for every individual query would be a significant operational impediment to legitimate investigations with serious negative public safety consequences. Other legitimate users of WHOIS data share similar concerns on specifying a legitimate interest for every query as it would impede their ability to ascertain the identities of responsible parties engaged in widespread online infringing activity.

The GAC therefore encourages ICANN to continue seeking clarification from the EDPB to ensure that access is proportionate to authenticated users' needs, not limited to individual lookups, and that access to WHOIS data for authenticated users is available in accordance with the specified purposes of the particular user group.

The GAC welcomes ICANN's acknowledgement that, under the UAM, Contracted Parties would be required to provide data for authenticated users. ICANN should train and resource their compliance team to ensure that the Contracted Parties are granting access in line with the UAM.

The GAC believes that, in line with the EDPB letter referenced on page 12, any logging and audit practices needed for transparency should come with appropriate safeguards to ensure non-disclosure of legitimate law enforcement activities. Confidentiality is needed not just in disclosure to the registrant, as discussed above, but also in sharing any logs with any outside parties, including ICANN. The UAM must balance data subjects' rights with legitimate law enforcement needs for confidentiality.

Regarding the searchability of non-public WHOIS records (i.e., cross-referencing of records), the GAC reiterates the public safety importance of this feature in identifying and mitigating DNS abuse. Since this is already a possible feature in RDAP, it deserves inclusion in the UAM, at least for certain user groups, subject to appropriate data protection safeguards, including measures to ensure a sufficient degree of compliance assurance.

Given the public interest and public safety use of WHOIS data, the GAC does not recommend requiring fees and thereby restricting access to public safety organizations. This is of particular concern in low-income countries and small, local law enforcement agencies.

Technical Details (Questions 11-13)

Regarding technical details under the Summary Description of a Framework for a Possible Unified Access Model (*Id.* at 13-14), the GAC welcomes the consideration given to ways of making the model more user-friendly, such as through a centralized lookup portal.

The GAC calls for further consideration of what these options would imply in terms of (international) data flows, how the system would work, and of what the potential technical, security and legal implications for such a system would be, noting that a central repository would imply a major shift with respect to the current system.

The current fractured nature of access to non-public WHOIS data amongst all registrar and registry operators creates confusion, increases the burden on investigators, slows investigations, and is technically harder for the Contracted Parties to maintain and operate.

Terms of Use (Questions 14-19)

Regarding the terms of use for accessing non-public WHOIS data under the Summary Description of a Framework for a Possible Unified Access Model (*Id.* at 14-16), the GAC believes that any common safeguards developed by ICANN that are common across all Terms of Use should not supersede legal requirements or obligations in each respective country.

The GAC recognizes that law enforcement agents often need to conduct multiple queries, such as when identifying or mitigating a large-scale botnet threat. In that view, the GAC acknowledges that rate limiting could be a significant operational impediment to legitimate investigations.