Framework Elements for Unified Access Model for Continued Access to Full WHOIS Data – For Discussion

18 June 2018
Prepared by: ICANN organization

This paper is a working draft document intended to facilitate discussions about 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 the European Union's General Data Protection Regulation (GDPR). The approach suggested in this paper is a starting place for further discussions with the community.

Background

On 17 May 2018, the ICANN Board adopted the Temporary Specification for gTLD Registration Data (Temporary Specification). The Temporary Specification establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. The Temporary Specification maintains robust collection of Registration Data (including Registrant, Administrative, and Technical contact information), but restricts most personal data to layered/tiered access. Users with a legitimate and proportionate purpose for accessing the non-public personal data are able to request such access through gTLD registrars and registry operators.

In view of the layered/tired access approach in the Temporary Specification, ICANN org's publication of the (1) Proposed Interim Model for GDPR Compliance – Summary Description (the "Calzone Model", 28 February 2018), and (2) Interim Model for Compliance with ICANN Agreements and Policies in Relation to the Union's General Data Protection Regulation (the "Cookbook", 8 March 2018) included some initial thinking about a proposed approach for providing continued access to Thick WHOIS data. Additionally, various parts of the community, including governments and European Data Protection Authorities have called for community work to develop a unified approach for accessing non-public WHOIS data. For example, in its 11 April 2018 letter, the Article 29 Working Party stated that 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. In this respect the WP29 encourages ICANN to develop appropriate policies and procedures applicable to incidental and*

> *systematic requests for access to WHOIS data, in particular for access by law enforcement entities.*[1]

Also, the European Commission invited ICANN "to consider and possibly integrate models for the accreditation system currently being developed by relevant stakeholders (e.g. by the business community). ICANN should take this opportunity to come up with a model that reflects not only compliance with the GDPR, but a genuine commitment to the spirit of the GDPR. At the same time, ICANN should be proactive, and ensure that the system will actually operate to mitigate risks of potential or actual harm to people and the security and stability of the Internet. This is a core part of ICANN's mission."[2]

This paper outlines a possible unified approach to allow continued access to full WHOIS data for authenticated users with a legitimate interest consistent with the GDPR. In summary, the approach could provide access to full WHOIS data to public law enforcement and other governmental authorities recognized by governments, and to defined categories of private third parties who are bound to abide by codes of conduct requiring adequate safeguards and measures of protection for personal data made available to the authenticated user.

The proposed approach attempts to provide an alternative uniform method beyond legal due process for registries and registrars to provide continued access to full WHOIS data for legitimate purposes, but recognizes that such an approach may prove to be challenging given the legal parameters of the GDPR requiring the balancing of legitimate interests with the interests, rights, and freedoms of affected data subjects. Developing a unified approach for proportionate data processing consistent with the GDPR while minimizing the risk of unauthorized and unjustified processing will require careful consideration and consultation with the relevant data protection authorities to develop a legally sustainable solution.

This document provides high-level framework elements to be addressed in a proposed 'Unified Access Model'. For each element, a recommended approach is provided for discussion with relevant governments, data protection authorities, and the community. Other parts of the ICANN community also are working on possible approaches for a unified method (or accreditation method) to provide continued access to full WHOIS data, and these community-developed approaches have been considered in the drafting of this document. A comparison chart of the various proposals submitted to ICANN[3] has been provided on ICANN org's Data Protection/Privacy Issues page (https://www.icann.org/dataprotectionprivacy).

[1] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf

[2] https://www.icann.org/en/system/files/correspondence/viola-et-al-to-marby-17may18-en.pdf

[3] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en#icann-models

Eligibility

1. Who would be eligible for continued access for WHOIS data via the Unified Access Model?

Only a defined set of user groups with legitimate interests who are bound by codes of conduct requiring adequate measures of protection would be eligible for access to non-public WHOIS data via the Unified Access Model.

Registry operators and registrars would continue to be required to provide reasonable access to other third parties on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR.

2. Who would determine eligibility?

At the outset, governments within the European Economic Area (who also are members of the GAC) would identify or facilitate identification of broad categories of eligible user groups ("Eligible User Groups"). Building from this guidance, ICANN org would engage with other governments through the GAC to identify specific Eligible User Groups. For example, Eligible User Groups might include intellectual property rights holders, law enforcement authorities, operational security researchers, and individual registrants.

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

For law enforcement authorities, individual governments would determine authentication requirements for who should be granted access from their respective jurisdictions. This information would be communicated via the GAC. As noted in the 11 April 2018 letter[4] from the Article 29 Working Party, there could potentially be a role for Interpol or Europol to serve as the global body to help determine the authentication requirements for law enforcement authorities. The Article 29 Working Party notes that, "[t]he 'accreditation' for incidental or systematic access to WHOIS data by law enforcement agencies might be arranged through for example Interpol or Europol, to help registries and registrars globally to ascertain the accreditation of such an agency, provided this can be done in accordance with the applicable legal frameworks."[5] ICANN org has requested additional clarification from the Article 29 Working Party (now European Data Protection Board) about the "applicable legal frameworks" referenced in the 11 April letter. For example, it would be helpful to understand, for example, whether the tasks for Europol established in Article 4 of the Regulation (EU) 2016/794 on the

[4] https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf
[5] https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf

European Union Agency for law Enforcement Cooperation could possibly serve as the legal justification for Europol to act as the body for determining authentication requirements for law enforcement authorities.

Also, ICANN seeks to understand more clearly whether, and if so how, Interpol or Europol could possibly qualify under Article 41 GDPR as a "body which as an appropriate level of expertise" for monitoring compliance with proposed codes of conduct for accessing non-public WHOIS data, considering the purpose and objective of Art. 41 GDPR in context of the GDPR as a whole.

For private third-parties, ICANN would consult with the GAC on identifying relevant bodies with expertise to authenticate users within an Eligible User Group (the "Authenticating Bodies"), and the Authenticating Bodies would develop criteria to authenticate individual users within an Eligible User Group.

If the GAC is unable to assist in identifying Authenticating Bodies, ICANN would work with the broader community to identify such groups. Some parts of the community have begun discussions in this regard, and for example, have identified WIPO or a similar party as the administrator of the Trademark Clearinghouse as possible Authenticating Bodies for intellectual property rights holders.

Additionally, there would be specific user groups who are automatically approved for access via the Unified Access Model for specific legitimate purposes – namely, ICANN for the purpose of contractual compliance enforcement, and registrars for the purpose of facilitating the transfer of domain names.

Process Details

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

Both registry operators and registrars would be required to provide access to non-public WHOIS data under the Unified Access Model to authenticated users.

Discussions about whether only registrars should be required to provide access to non-public WHOIS, for example, would be a possible topic for discussion in any relevant policy development process.

5. What would be the overall process for authenticating legitimate users for access non-public WHOIS data under the Unified Access Model?

A third party with a legitimate interest for accessing non-public WHOIS data would submit to the approval process required by the relevant Authenticating Body, which could include an application process for example. If the user successfully satisfies the requirements of the Authenticating Body, the user would be required to confirm its adherence to the relevant Code of Conduct, which is discussed in additional detail below.

Two potential approaches are proposed for discussion about who would provide authenticated users the required credentials to access non-public WHOIS data:

- **Option 1**: The Authenticating Body would direct the user to a centralized “credential provider” who would grant the user the required token/credential to be presented to the registry operator or registrar to access non-public WHOIS data; or

- **Option 2**: The Authenticating Body would itself provide the required token/credential to be presented to the registry operator or registrar to access non-public WHOIS data.

To gain access to the non-public WHOIS data, the authenticated user would present its token/credential to the relevant registry operator or registrar and identify its legitimate purpose for requesting access to the non-public WHOIS data. The registry operator or registrar would evaluate the request, and the authenticated user would be provided query-based access to non-public WHOIS data as appropriate.

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

ICANN org would seek guidance from the European Data Protection Board on two possible approaches for the scope of data that would be available to authenticated users:

- **Option 1**: The Authenticated users would be granted query-based access to the level/scope of non-public WHOIS data consistent with the identified legitimate purpose presented to the registry operator or registrar for each query.

- **Option 2**: The Authenticated users would be granted query-based access to the full WHOIS record for each query.

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

Registry operators and registrars would be required to provide global access to authenticated users consistent with the identified legitimate purpose, and subject to applicable local laws.

8. Would the Unified Access Model incorporate transparency requirements?

Yes, the Unified Access Model would incorporate transparency requirements. For example, each Authenticating Body or the centralized “credential provider” (see Question 5) would maintain a list of the authenticated users.

Additionally, based on initial discussions with members of the Article 29 Working Party, ICANN proposes that registry operators and registrars would be required to maintain audit logs of domain name queries for non-public WHOIS data, unless logging a particular entry is contrary to a relevant court order. The logs would be available to ICANN org for audit/compliance purposes, relevant data protection authorities, the registrant, or pursuant to a court order. ICANN is seeking further guidance from the European Data Protection Board on this point to understand what appropriate logging and auditing mechanisms should be incorporated into the Unified Access Model. (See https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf).

9. Would there be any fees as part of the Unified Access Model?

Accreditation models for access to non-public WHOIS data presented by some community members include the possibility of application fees and/or nominal fess to access non-public WHOIS data. The financial implications of the Unified Access Model would require further study to assess this issue.

10. Would there be a process to review the effectiveness of the Unified Access Model?

Yes, the Unified Access Model would be reviewed at regular intervals to identify efficiencies and improvements to the implementation of the model.

Technical Details

---

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

No, registries and registrars would maintain current requirements to operate a WHOIS service.

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

Registry operators and registrars would be required to provide access to non-public WHOIS data via a Registration Data Access Protocol (RDAP) service.

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

The Unified Access Model would rely on a system of tokens and/or certificates as the technical method for identifying authenticated users.

Codes of Conduct for Accessing Non-Public WHOIS Data

14. What would be the role of Codes of Conduct in the Unified Access Model?

Codes of Conduct would establish a framework for the use of non-public WHOIS data by third parties and in particular appropriate limitations on the use of such data, proper procedures for accessing the data, and other safeguards and public policy considerations relating to the responsibilities and practices for the Eligible User Groups.

In general, the non-public WHOIS data must be used for the purposes it was provided, and it must not be forwarded to unauthorized third parties.

15. Would there be multiple Codes of Conduct?

Yes, the Unified Access Model would include separate Codes of Conduct for each Eligible User Group to pursue a tailored and balanced approach regarding these groups and taking into account differing user interests. There would therefore be some safeguards that are common across Codes of Conduct, whereas other safeguards would be specific to the Eligible User Group.

16. How would the Codes of Conduct be developed?

In consultation with the GAC and the European Data Protection Board, ICANN org would develop the standardized terms and safeguards common across each Code of Conduct.

The Authenticating Body for each Eligible User Group would be responsible for developing additional safeguards specific to the relevant Eligible User Group, which would be incorporated in the Code of Conduct.

17. What types of safeguards would be included in the Codes of Conduct?

Among other things, the Codes of Conduct would include the following types of safeguards:

a. Appropriate limitations on use of the data;
b. Proper procedures for accessing the data, including appropriate limitations on query volume to prevent abuse;
c. Security measures for accessing the data;
d. Limitations on onward transfers of the data;
e. Safeguards for data subject rights;
f. General data protection obligations of the data controllers;

g. Fair and transparent processing requirements; and
h. Other safeguards and public policy considerations relating to the responsibilities and practices for the Eligible User Group.

18. What mechanism would be used to require compliance with the Codes of Conduct?

Authenticated users would be required to declare adherence to the relevant Code of Conduct, either through an agreement with the Authenticating Body or some other method binding the user to comply with the Code of Conduct.

19. Who would monitor and enforce compliance with the Code of Conduct?

The Authenticating Body would monitor and enforce compliance with the relevant Code of Conduct. ICANN org would develop a Memorandum of Understanding or Agreement with each Authenticating Body to ensure appropriate oversight consistent with ICANN's mission stipulated in the Bylaws.

Compliance issues concerning registry operators' or registrars' adherence to the requirements of the Unified Access Model would continue to be handled by ICANN's Contractual Compliance department.

Next Steps/ Timing

ICANN org looks forward to the discussions around this draft, and will continue engaging in the process of community consultations, including with the European Data Protection Board and governments, about a proposed Unified Access Model. Input from the community will be important to contribute to further refine the Unified Access Model. Overall, ICANN org proposes to organize the work into three phases as follows:

- Phase 1: Community discussion and consultations on the Unified Access Model
- Phase 2: Consultation with the European Data Protection Board on the Unified Access Model and the approach to develop Code of Conducts for various Eligible User Groups
- Phase 3: Further refinement and finalization of the Unified Access Model based on inputs from the community and the European Data Protection Board

Also to note, as required by the Temporary Specification for gTLD Registration Data, registries and registrars are required to implement the technical protocol (RDAP) by mid-December 2018, which will enable the implementation of the final Unified Access Model when it is available.