12 April 2019 Submit to: gdpr@icann.org

InfoNetworks Comments to the Draft Technical Model for Access to Non-Public Registration Data

InfoNetworks appreciates the opportunity to comment on the Technical Study Group's *Draft Technical Model for Access to Non-Public Registration Data*. We commend the TSG for their consideration of the differing concerns of numerous constituencies across the community and their efforts in developing a Technical Model to support the wide variety of legitimate purposes for which non-public registration data is used.

Over the past several years, InfoNetworks has been engaged in an in-depth, global review of regulatory approaches to consumer privacy and data sovereignty—considering not just technical models, but also approaches to the underlying governance (policy and legal frameworks) upon which any technical model must be built. We have conducted our analysis as specifically applied to managing access non-public registration data, as well as to "digital identity" and solutions for the exchange of personal data in online transactions more generally.

The comments provided herein are based on that work and our review of the current draft of the requirements for the Technical Model. We are hopeful that the TSG will find our comments of value for refining those requirements as the larger governance discussion continues.

Decisions on governance will be determinative of GDPR compliance

In the Executive Summary for the Technical Model, the TSG indicates that ICANN asked them to "explore an implementation approach that would place ICANN as the funnel for third-party queries for non-public registration data in the gTLD space.… to help ICANN org determine whether such a model would diminish the legal liability for gTLD contracted parties…"

But notably, the group's charter precluded consideration of any "decisions or recommendations on policy questions" and does not present any assumptions as to contractual terms or other legal mechanisms, all of which will (along with a supporting Technical Model) ultimately determine whether a unified model for managing access to non-public registration data is compliant with various data privacy regulations, including but not limited to the GDPR, as well as the legal liability of a Contracted Party if the privacy rights of a data subject are infringed.

We recognize that the TSG, in drafting its proposal, appropriately assumed that "[p]olicy choices may change the technical implementation of the proposed draft technical model." However, we believe that—as stated—this significantly understates that decisions on governance will, in fact, be largely determinative of whether a unified access model is GDPR compliant and will materially impact the legal liability of the Contracted Parties, whereas a Technical Model, in and of itself, will not.

Compliance with data privacy regulations like the GDPR fundamentally depends on governance—policies, contractual terms, and other legal mechanisms among the relevant parties, and not on particular technologies or technical approach *per se*. This is made clear in the opening text of the GDPR: "In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral ***and should not depend on the techniques used***."[1]

The GDPR requires that a controller "shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" and, when appropriate, these "shall include the implementation of appropriate data protection ***policies*** by the controller."[2]

The GDPR goes on to require that "the controller shall use only processors providing sufficient ***guarantees*** to implement appropriate technical and organisational measures." This includes that "a processor shall be ***governed by a contract or other legal act*** … that sets out the … obligations and rights of the controller" and that the processor processes "the personal data only on documented instructions from the controller."[3]

The GDPR does recommend several technical measures: pseudonymisation; availability and resilience of processing systems and services; access to personal data in a timely manner in the event of a physical or technical incident; and regular testing the effectiveness of technical measures.[4] However, the GDPR intentionally does NOT specify particular technology frameworks, as specific technical implementations must take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons."[5]

To illustrate this point, we note that the draft Technical Model does not provide a rationale for requiring that "all queries are directed and all responses are filtered" through a central ICANN gateway; and it is unclear how such a technical requirement would meaningfully reduce the legal liability of the Contracted Parties or support GDPR compliance.

An ICANN gateway would not, *ipso facto*, reduce the legal liability of Contracted Parties

As highlighted in the *Draft Framework for a Possible Unified Access Model*, the EDBP noted in their letter of July 5, 2018 that "ICANN and the registrars/registries are, ***as controllers***, responsible for ensuring that personal data processed in the context of WHOIS are only disclosed to third parties with a legitimate interest or other lawful basis" and that "[t]he responsibility for designing a model that will provide this assurance is in the first instance ***up to ICANN and the registrars/registries***."

[1] Paragraph (15) of the GDPR's opening recitals.

[2] Article 24 of the GDPR.

[3] Article 28 of the GDPR.

[4] Article 32 of the GDPR.

[5] Article 24 of the GDPR.

Any controller[6] or processor who is involved in processing that results in damage to a data subject "shall be held liable for the ***entire*** damage." Once a party has paid the ***full*** compensation to the data subject, that party can claim back from the other liable parties the portion for which they were not responsible. However, the GDPR also provides that a controller or processor is liable where it has not complied with the ***obligations*** under the GDPR for which it is specifically responsible—unless that party proves that it is not ***in any way responsible*** for the event harming a data subject.[7]

Under the currently proposed Technical Model, a Contracted Party would still be processing the requested personal data via RDAP and would "assume that ICANN will ensure validity of credentials." A Contracting Party's legal liability (as a controller or a processor) to a data subject would thus turn on demonstrating that it was not responsible, in any way, for the harm suffered by a data subject by virtue of it fulfilling a request for their personal data.

Every request for personal data requires a Contracted Party to process data controlled by that Contracted Party, and it is not clear how adding ICANN "as the funnel for all third-party queries" would, in and of itself, mitigate a Contracted Party's responsibility for processing that data.

We are also unaware of any provision within the GDPR itself by which processing through a central gateway would, in and of itself, change the parties' respective obligations. What the GDPR does provide is that parties can restructure their obligations by contract or other terms governing their relationship. For example, where two or more parties are joint controllers, they shall:

> … determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, ***by means of an arrangement between them*** unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.[8]

Thus, the legal liability of the Contracted Party would appear to be primarily dependent on the governance framework implemented by ICANN and the community—irrespective of whether all of the personal data is also processed through an ICANN gateway.

Related to this point, it is our understanding that ICANN does not wish to indemnify the Contracted Parties contractually. It is highly likely that the lack of any indemnification by ICANN coupled with a Contracting Party assuming that ICANN acted properly (without any regular testing or other verification of that process) would be a significant consideration in determining whether a

[6] The GDPR defines a "controller" as any party that "determines the purposes and means of the processing of personal data" and a processor is any party "which processes personal data on behalf of the controller." If a processor determines the purposes and means of processing the personal data (any processing), "the processor shall be considered to be a controller in respect of that processing." (Article 28 of the GDPR)

[7] Article 82 of the GDPR. A processor is otherwise only liable if it has acted outside or contrary to lawful instructions of the controller.

[8] Article 26 of the GDPR.

Contracted Party was still responsible, in some way, for the harm that a person suffered from a request that the Contracting Party fulfilled under this approach.

If the TSG is aware of a different interpretation of the GDPR that supports the view that a central gateway will, in fact, reduce the legal liability of the Contracted Parties, we suggest that it be added to the enumerated assumptions upon which the Technical Model is based—so that the community can better understand the rationale for this technical requirement.

The Technical Model should retain decentralized access

Absent a supporting rationale for a central gateway, it may be more beneficial to structure the technical requirements as originally envisioned, to enable alternative means for processing the data within a policy and legal framework that is an extension of the existing governance model for the domain name system.

While the Draft UAM Framework noted a suggestion for a central gateway (or even a centralized a WHOIS database), it assumed decentralized processing using federated credentials:

> "To gain access to the non-public WHOIS data, the authenticated user would present its credentials 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 verify the credentials with the Authenticating Body, evaluate the request, and the authenticated user would be provided query-based access to non-public WHOIS data as appropriate."

ICANN also noted in the Draft UAM Framework that it:

> … continues to separately explore whether there are "opportunities for ICANN, beyond its role as one of the 'controllers' with respect to WHOIS or its contractual enforcement role, to be acknowledged under the law as the ***coordinating authority*** of the WHOIS system."[9]

The Draft UAM Framework appropriately focused on the central role of ICANN as a coordinating body for the governance of a unified access model: accreditation, authentication, authorization, terms of use, access agreements, and adoption of a consensus policy or contract amendments.

While we recognize the potential significance of ICANN's role as a coordinating body under an appropriate governance framework, we are not aware of any provision in the GDPR (or any indication from the EDBP) under which a technical requirement for a central ICANN gateway would obviate a Contracted Party's legal obligations as a controller, or otherwise inherently shift those obligations to ICANN.

[9] Section D of the Draft UAM Framework, citing ICANN's blog post from 05 June 2018, *Data Protection/Privacy Update: ICANN's GDPR Efforts with Temporary Specification Now in Effect*

Added to this are significant potential performance, reliability, scalability, cost, and security concerns with adopting a centralized gateway for processing of all requests for non-public registration data. The TSG itself appropriately notes this concern:

> The TSG recognises that it is proposing a solution that could potentially impose ***significant operational burdens*** on the ICANN organization, especially if the community determines that the operator of the RDAP proxy must meet a stringent Service Level Agreement, and operate at significant scale.
>
> It is RECOMMENDED that the ICANN organization review the spectrum of potential operational outcomes for deployment and operation of the system proposed, to determine the ***feasibility*** of such outcomes, their ***operational and financial impact***, and how challenges might be addressed.
>
> It is RECOMMENDED that ICANN org publish its review for public comment and that it solicit feedback from technical experts on its ***feasibility***.

Proposed Revisions

For at least the reasons set forth above, we suggest that the draft Technical Model be revised along the lines of the following:

> **Executive Summary**
>
> …Rather, the work of the group is intended to help ICANN org determine whether such a model would diminish the legal liability for gTLD contracted parties, who would provide access to non-public registration data, when considered in conjunction with the policy and legal governance framework upon which such a model must ultimately be based.
>
> Building on the technology available via the Registration Data Access Protocol (RDAP), this approach would position ICANN as the ~~sole access point to~~coordinating body for non-public registration data. …
>
> The technical model would support a process that would allow users to verify their identity and legitimate purpose for requesting data, come to a ~~central~~ service managed by ICANN, and receive approval or denial of the request.
>
> **2.1 Other Terms**
>
> ~~ICANN~~ RDAP Access Service - A browser-based, web service used by the requestors to obtain an access token from the OAuth/OpenID Connect process. In OAuth/OpenID Connect terms, this would be the Relying Party….

~~ICANN~~ RDAP Gateway - An ~~central~~ RDAP proxy server through which ~~all~~ queries are directed and ~~all~~ responses are filtered.

3. Assumptions

3. ICANN will be the sole party for coordinating~~through which~~ access to non-public registration data is obtained in the gTLD space as part of a unified access model….

10. ~~Data holders assume that~~ ICANN will ensure validity of credentials.

4.1 User Journey

- Authorization is centralized within ICANN. Access of GDPR-protected data is ~~centralized within~~centrally managed by ICANN.

5. System Requirements

1. Overall…

   c. The system MUST support a distributed data model, where data is stored by the authoritative contracted parties and non-public data is only transferred through parties authorized by ICANN.

4. ~~ICANN~~ RDAP Gateway

7. Actor Models

2. ~~ICANN~~ RDAP Gateway - an ~~central~~ RDAP proxy server through which ~~all~~ queries are directed and ~~all~~ responses are filtered.

4. ~~ICANN~~ RDAP Access Service - A browser-based, web service used by the requestors to obtain an access token from the OAuth/OpenID Connect process. In OAuth/OpenID Connect terms, this would be the Relying Party.

5. ~~ICANN~~ RDAP Gateway - an RDAP server proxy evaluating access based on an access token to which ~~all~~ queries are submitted and through which ~~all~~ responses are filtered. In OAuth/OpenID Connect terms, this would be the Resource Server.

9. Proposed Solution

The authentication mechanism used between the client and anthe ICANN RDAP proxy will be based on OpenID Connect and OAuth 2.0 using either shared secrets (e.g., usernames and passwords) or digital certificates at the mutual choice of the Identity Provider and the client. …

Mutual TLS authentication will be used to secure RDAP communications betweenamong ICANN and the Contracted Parties, and also betweenamong subsystems. This method is recommended because ICANN and the Contracted Parties areis fully authorized for access to non-public data, and the Contracted Parties only need to authenticate ICANN themselves without having to make detailed authorization decisions on a per-query basis. The functional requirements not met by this method do not apply to interactions between ICANN and the Contracted Parties.

9.2 Processing Steps

1. Access Request

The requestor who wishes to perform an RDAP query uses an RDAP USer Agent to send an HTTP Access Request to thean Access Service. The Access Service will be operated by ICANN, a Contracted Party, or their authorized delegate. The Access Service receives the request and returns an HTTP redirect to the client that prompts the client to send an Authentication Request to an Authorization Endpoint operated by an Identity Provider.
…

3. Setup for RDAP Query

…

The client prepares an RDAP query. The RDAP query, an ID token, and an OPTIONAL Access token are sent to the ICANN RDAP Gateway.

4. RDAP Query Processing

The ICANN RDAP Gateway receives the RDAP query, an ID token, and an OPTIONAL Access token. The ICANN RDAP Gateway sends this information to a Third Party Authorizer (this service can also be operated by ICANN) for verification and validation. The tokens are validated as described in Sections 3.1.3.7 and 3.1.3.8 of the OpenID Connect specification, and the identity attributes (known as "claims" in OAuth 2.0) are retrieved from the ID token. The Third Party Authorizer maps the set of claims to a set of policies to determine if the requestor is authorized for access to any non-public data elements. The Third Party Authorizer sends a response to the ICANN RDAP Gateway that indicates the result of authorization processing. If the requestor is authorized, the ICANN RDAP Gateway sends RDAP queries to the specific contracted party RDAP servers that are authoritative (i.e., have the closest relationship to the data subject) for the individual

data elements within the requested data. These queries from the ~~ICANN~~ RDAP Gateway to the contracted party servers may contain secure metadata as specified by the system requirements and relevant policy. The contracted party RDAP servers each return RDAP responses containing the full set of data elements for which they are authoritative, which are received, processed, and filtered by the ~~ICANN~~ RDAP Gateway to form a complete RDAP response that contains non-public data in accordance with the requestor's level of access. The ~~ICANN~~ RDAP Gateway returns the RDAP response to the client.

10.2 Service Level Agreements (SLAs)

…

- ICANN org (as an~~the~~ operator of an~~the~~ RDAP Gateway)

Conclusion

While there are definite benefits to using a single access portal to consolidate an RDAP request for non-public registration data across multiple authoritative sources, this does not mean that it is necessary to have a central gateway managed by ICANN. This is particularly true with the adoption of federated credentials. With the appropriate governance model in place, a number of authorized access points could exist into an RDAP ecosystem among the Contracted Parties, whether provided by Contracted Parties themselves, ICANN, or others. When the

For the reasons set forth above, we believe that the Technical Model should enable such alternatives.

Sincerely,

Frank A. Cona

Michael D. Palage