February 25, 2018

By Electronic-Mail

Akram Atallah
President, Global Domains Division
Internet Corporation for Assigned Names and Numbers

John Jeffrey
General Counsel and Secretary
Internet Corporation for Assigned Names and Numbers

Re: Initial Feedback on ICANN's "Convergence Model."

Dear Akram and John:

Thank you for taking the time to join the GDPR discussion hosted by the IPC on February 22nd and for discussing key high-level elements of ICANN's "Convergence" Model (the "Model"). We are encouraged by much of the high-level decision points that you described as being contained in that Model. In particular, we fully support ICANN's articulated decisions:

(1) that, short of DPA okay or approval otherwise, the contracted parties should not be required to publish email addresses as part of a publicly available minimum WHOIS data set (but will still be included in a credentialed/gated WHOIS system);

(2) that contracted parties should not be required to publish different sets of WHOIS data based upon a self-identified distinction (by the registrant) between natural and legal persons; and

(3) that contracted parties should apply the Model globally, as opposed to segmenting the WHOIS based upon where a registrant self-identifies as being located.

The inclusion of these fundamental elements in the Model represent a positive and constructive step towards an implementable model and we welcome them. We look forward to seeing, in greater detail, the full text of the Model. While we see the inclusion of these high-level principles into the Model as positive developments and evidence of the benefits of our increased collaboration, there are still many unanswered questions that must be quickly and specifically addressed.

Most significant are those questions revolving around the concepts of credentialed or gated access to WHOIS data. In particular:

(1) *How will credentialing work*?

ICANN signaled on the Thursday 22 February, call that the Model will consider a mechanism for credentialed or gated access. While credentialed or gated access to the WHOIS is certainly more defensible than a publicly open WHOIS, what that system looks like will

ultimately make all the difference for GDPR compliance. Who can access and under what circumstances/criteria are critical questions yet to be determined.

(2) *A centralized credentialing body?*

If ICANN is contemplating a central credentialing body, can it share its thoughts as to what that might look like? Specifically:

- What body will perform the credentialing?
- Will uniform criteria used by the credentialing body in making a determination to grant a credential be published?
- Would there be one credentialing body for all gated WHOIS access, or separate credentialing bodies for different purposes (e.g., one credentialing body for security research purposes and one credentialing body for intellectual property rights holders)?

(3) What is the "Interim for the Interim" for Credentialing?

While a central credentialing body is desirable for contracted parties and those seeking to make WHOIS requests, having such an entity/organization and the requisite technical development operationalized in the next three months is unlikely. If that is the case, and the Model still contemplates a mechanism for credentialed or gated access, it leaves a substantial void that would need to be filled by an immediate "Interim for the Interim" solution to deal with how we limit access to some appropriate level of degree. We could not support an immediate interim solution that relies upon a pure "Self-Certification" method to gain access to nonpublic WHOIS, unless and until a Data Protection Authority clearly states that self-certification is acceptable for that purpose. Without such an assurance, self-certification on its own is not defensible as it amounts to an "honor system" that can and would be easily gamed by any actor seeking to access the non-public WHOIS (i.e., it serves as no true gate at all).

At a bare minimum, any immediate interim solution should include both (1) validation of the identity and standing of the requesting party and (2) self-certification for before access to non-public WHOIS is granted. This would create essentially a two-factor authentication system before a requesting party is allowed in "behind the gate" and allow them to conduct searches of the non-public WHOIS. That party would then be required to abide by terms of service which would prohibit use of data gained in these searches in a manner that is inconsistent with the GDPR. For example, in addition to the requestor having to provide a self-certification prior to making a request to access to non-public WHOIS, that requestor might also need to be validated by an independent third party, perhaps selected in consultation with its respective constituency, prior to gaining access behind the "gate." In this scenario, the independent third party would work with the IPC to provide a credential for a requesting entity to gain access in order to enforce an existing intellectual property right. The credential would then be supplied to the contracting party where the requestor is seeking to gain access to the non-public WHOIS. That additional step of confirming the proper identity of the requesting entity and that it has some

colorable claim to the legitimate interests it is asserting with regards to its request makes self-certification more defensible.

(4) What is available Behind the Gate?

Once a credentialed entity or individual has access to the WHOIS, what can it access? Is its access limited to searches for particular domain names or may it have bulk (port 43 equivalent) access? While we understand that some WHOIS users consider the ability to search across an entire database is critical, we are concerned that this kind of access is in tension with both the purpose limitation principle and the data minimization principles required by Art. 5 of the GDPR. We believe that DPA guidance on this point is required. Similarly, what happens if a requestor is found to have abused its access to the non-public WHOIS? It seems to follow that any requestor would have to agree to some terms of service ensuring that it will access, collect, retain and delete any data in the non-public WHOIS in a manner that is consistent with the GDPR.

Please note that these are simply some initial reactions to the Convergence Model and not a complete analysis. Given the speed of developments in recent weeks, however, we thought it important to share our immediate impressions and receptiveness to the tenets first outlined above. We look forward to further discussions on these questions and hearing more about the Model.

Sincerely yours,

Paul Diaz, RySG Chair
Graeme Bunton, RrSG Chair

cc: Göran Marby, CEO