ICANN Contracted Party and Intellectual Property and Business Stakeholders
WHOIS Access and GDPR Compliance Interim Model Discussion Group

February 21, 2018

COMMUNIQUÉ

I. Introduction

Surrounding the Non-Contracted Parties House (NCPH) Intersessional held in Los Angeles February 1 – 2, 2018, the ICANN CEO made a request to leaders from the ICANN contracted party community and the intellectual property and business stakeholders communities to hold direct discussions regarding an interim model for compliance with the European General Data Protection Regulation (GDPR), while preserving as much of the current WHOIS system as possible. This meeting is the product of that request, and the general recognition of the need for direct dialogue to develop an interim compliance model that is acceptable for contracted parties and WHOIS users.

Members of the participating stakeholder communities agreed on the following principles and priorities to guide their discussion:

- That constructive communications across constituencies are important for moving the conversation forward on these important issues;
- That a uniform compliance model developed as a result of cross-constituency collaboration is much preferred to the implementation of divergent models with inconsistent principles; and
- That the discussion and development of specifics around the tiered/gated access model and the credentialing process are critical.

Please find below a discussion of areas of agreement and divergence determined during the meeting, as well as areas flagged for further work and discussion.

II. Participants

The in-person meeting took place on Wednesday, February 21, 2018 from approximately 12 pm to 5 pm Eastern (US) time. The meeting participants included:

Representing Contracted Party Stakeholders:

James Bladel, GoDaddy

Kevin Kreuser, GoDaddy

Graeme Bunton, Tucows

Beth Bacon, Public Interest Registry

Brian Cimbolic, Public Interest Registry

Samantha Demetriou, Verisign

Rahael Seifu, Google

Becky Burr, Neustar

Representing Intellectual Property and Business Stakeholders:

Brian Winterfeldt, Winterfeldt IP Group

Vicky Sheckler, Recording Industry Association of America

Patrick Charnley, IFPI

Margie Milam, Facebook

Tim Chen, DomainTools

Fabricio Vayra, Perkins Coie

Susan Kawaguchi, CNA Consulting

Observing as ICANN Board Members:

Sarah Deutsch

Ron da Silva

This group was not intended to be fully representative of the various stakeholders affected by ICANN's GDPR compliance model, nor should any of its discussions or conclusions be read as binding commitments on the part of any individual, group or constituency participating.

III. Areas of Agreement

A. Publish Registrant Organization (if any)

B. Publish Registrant State/Province

C. Publish Registrant Country

D. Publish all "thin" registration data

E. No need to collect and/or publish Administrative or Technical contact information unless either of these data sets diverges from the Registrant contact information (indicating the Registrant made a conscious decision to provide separate Administrative and/or Technical contacts).

F. If a Data Protection Authority were to affirmatively "bless" any particular facet of the status quo data elements of WHOIS, both the contracted party stakeholders and

intellectual property and business stakeholders would prefer to keep those status quo elements in place.

IV. Areas of Divergence

A. **Data Subject Applicability.** Differentiation between Natural and Legal Persons – attendees agreed that the GDPR makes this distinction and that the intent of the GDPR is to apply only to Natural Persons. However, while intellectual property and business stakeholders suggested such a differentiation could be easily implemented, contracted party stakeholders expressed significant concerns that there would be technological and policy implementation challenges – particularly because domain name contact information is normally provided by the Registrant, and this legal distinction is not widely understood.

B. **Territorial Applicability.** Differentiation of registrants and contracted parties within and outside the EU – the parties agreed that such differentiation comports with the territorial scope of the GDPR. However, while intellectual property and business stakeholders suggested such a differentiation could be easily implemented, contracted party stakeholders expressed serious concerns with implementation and scalability, and continue to question the legality of the status quo in other jurisdictions around the world.

C. **Registrant Email Address.** Publication of Registrant email address in WHOIS – intellectual property and business stakeholders offered that the Registrant email address could be a public data element in light of legitimate purposes, while contracted party stakeholders require assurances from European Data Protection Authorities that such publication would not violate GDPR requirements, given that Registrant email address would be personally identifiable information subject to the rules of the GDPR in many instances.

D. **Registrant City and Postal Code.** There was discussion and initial agreement to consider that the Registrant city and Registrant postal code data elements could be part of the public data set. Ultimately, because the participants did not have conclusive information regarding the impacts of publishing this data, due to global variations with respect to city and postal code data, the group could not reach internal consensus on this issue and publication of these data elements is therefore not included as an additional area of agreement. Instead, we mention it here as an area of divergence and potential item for continued exploration.

E. **Data Accuracy.** Data accuracy requirements – intellectual property and business stakeholders proposed that these should be expressly included in any interim compliance model, while contracted party stakeholders propose that the accuracy

principles of the GDPR do not equate to an obligation to verify each individual element of WHOIS information provided by the Registrant.

F. **Bulk Data Access.** Port 43 WHOIS access (bulk/aggregated access to WHOIS data) – intellectual property and business stakeholders proposed that such access is critical for various legitimate purposes, while contracted party stakeholders stated such access is likely in conflict with the GDPR's principle of data minimization, among others.

V. Areas Identified for Further Work and Discussion

A. Clarify whether any proxy service registration data would be published in WHOIS or any generally non-public data elements would still be non-public when they are the data of a proxy registrant. In any event, the public WHOIS database should include a separate data element to identify if the registration is made through a privacy or proxy service, per the adopted recommendations of the Privacy & Proxy Services Accreditation Issues Policy Development Process.

B. Possibility of implementing a unique pseudonymous email address in the public WHOIS that allows Registrant contactability with direct data accuracy technical feedback (e.g. email bounceback), and ability to use that unique but pseudonymous email address to correlate all domain names registered by a single registrant.

C. Develop proposals for interim self-certification plus credentialing ("self-certification plus") and/or third-party accreditation systems for legitimate purposes/users, specifically for cybersecurity, consumer protection, and intellectual property enforcement. In particular, intellectual property and business stakeholders are going to brainstorm how they would propose verifying/credentialing individuals or entities that seek access to non-public WHOIS data in furtherance of enforcing intellectual property rights, performing cybersecurity functions, and other legitimate tasks that rely on such data. Contracted party stakeholders also note that any accreditation system, whether interim or permanent, must include a process for reporting and/or revoking credentials that violate the legitimate purposes associated with the accredited user.

D. Clarify level of access to non-public WHOIS data once a party is accredited or otherwise permitted to access non-public data. For example, once permitted access, can the user access all non-public data in WHOIS? All non-public data for a specific individual WHOIS query? Access only to certain non-public data elements but not all non-public data?