INTELLECTUAL PROPERTY CONSTITUENCY COMMENTS ON PROPOSED INTERIM MODELS FOR ICANN COMPLIANCE WITH EU GENERAL DATA PROTECTION REGULATION

January 29, 2018

The Intellectual Property Constituency (IPC) of the Generic Names Supporting Organization (GNSO) is pleased to submit public comments on proposed interim models for compliance with ICANN agreements and policies relative to WHOIS in relation to the European Union's General Data Protection Regulation ("GDPR"). Although ICANN's request for input (the "Document") initially specified that it was seeking comments only on its three proposed compliance models, as prepared and published by ICANN Org on January 12, 2018 (the "ICANN Models"), ICANN has since clarified[1] that it is eager to receive input covering the ICANN Models as well as the five compliance models submitted by various community participants (the "Community Models"), including suggestions for "hybrid" models that draw from all the models and available legal analyses. Accordingly, the IPC's input considers all of the available models and analysis, and proposes a hybrid compliance solution that draws from these various sources.

Executive Summary

ICANN's goal of ensuring compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible can be best achieved through the adoption of a hybrid model that combines elements of ICANN Model 1 with two critical modifications: (i) including Registrant e-mail address in Public WHOIS, and (ii) adopting a true self-certification process for third-party legitimate interest access to non-public data. These elements are discussed in certain community models, most notably the model submitted by the Coalition for Online Accountability (COA).

The formal and standardized accreditation/certification proposal for third-party access to non-public data as proposed in ICANN Model 2 would be beneficial if it could be achieved in time.

ICANN Model 3 is unworkable from many stakeholder perspectives. It does not come close to achieving the stated compliance goal and would impose grave and unacceptable burdens on WHOIS users, contracted parties, and the court system and other public authorities. It should be excluded from any further consideration.

[1] On January 24, 2018, during an event on GDPR and WHOIS issues co-hosted by the IPC and ICANN Business Constituency (BC), the ICANN CEO and General Counsel clarified that ICANN would consider input on ICANN's compliance models, as well as those submitted by community members, as well as suggested "hybrid" models drawing from the other models under discussion.

Introduction

ICANN has repeatedly stated that its goal in pursuing interim solutions to meet the impending enforcement date of the GDPR (May 25, 2018) is to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible." ICANN explicitly set forth this objective in the Approach to Developing Interim Compliance Models section of the Document. We agree with and support this goal, which is consistent with ICANN's Mission, as well as ongoing efforts to reduce and deter abuse of the DNS. We also agree with ICANN org's statement in the Document that the selected interim model "will not replace the multi-stakeholder policy development and implementation activities that are underway" to address these and related issues beyond an interim basis.

We have identified three corollary principles that necessarily follow from the overall objective of ensuring compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible:

1. Scope: Limit modification of contractual WHOIS obligations to personal data that explicitly fall within the scope of the GDPR.

2. Public WHOIS: Maintain to the greatest extent possible the amount of data still available in Public WHOIS while complying with the GDPR.

3. Tiered Access: For data that is no longer available in Public WHOIS, adopt a tiered access system that: (i) minimizes burdens on both registrars/registries and third-parties with legitimate interests seeking access to such data, and (ii) provides for expedited access, reliability and consistency, while complying with the GDPR.

With the overall objective and these three corollary principles as starting points, we offer the following comments on the proposed interim compliance models.

Comments Common to the ICANN Models

A. Working Purpose Description: We support the statement of purposes that is proposed for the interim models as set forth on pages 5 and 6 of the Document and believe it appropriately and succinctly captures the array of registrant, registrar and registry, public interest and legitimate third-party interests and purposes for collecting and processing registrant data. As stated in our comments on the Hamilton legal analysis, we agree on the need to set forth more clearly and fully all the purposes for which WHOIS data is used and the legitimate interests served by access to such data.

B. Thin WHOIS Data: We support continued public access to all thin WHOIS data.

C. Consent: While consent should not be (and in fact is not) the sole basis for collecting and processing WHOIS data, we believe it is a relevant and useful avenue for maintaining personal data in Public WHOIS in compliance with the GDPR. Therefore, we support the requirement that registrars must seek "specific and informed consent that is freely

given, unambiguous [and] withdrawable at any time" as a means of publication of full thick WHOIS data.

D. Collection and Transfer to Registries of Thick WHOIS data: The Document provides that registrars "may" collect and "may" transfer to the relevant registry all Thick WHOIS data. This should be a required obligation consistent with existing ICANN contractual obligations and not merely a permitted option. Therefore "may" should be changed to "must."

E. Bulk Access: None of the models address the issue of bulk access to data in certain circumstances, which is critical to law enforcement, efforts to combat phishing and other online abuse, and intellectual property rights protection.[2] We support providing explicit guidance on how parties with legitimate interests who self-certify can gain broader access to WHOIS data in certain circumstances.[3]

F. Data Accuracy: In addition, none of the models address data accuracy, even though data accuracy is a fundamental principle of the GDPR. (See Article 5(d) of GDPR: "Personal data shall be: . . . accurate and, where necessary, kept up to date").

Comments on ICANN Model 1

Of the three interim models proposed by ICANN, ICANN Model 1 most closely fulfills the objective of complying with the GDPR while maintaining the existing WHOIS system to the greatest extent possible, and IPC supports its adoption subject to the following modifications below. In general, ICANN Model 1 provides a good balance between the interests of all stakeholders, and is most consistent with ICANN's mandate compared to the other ICANN Models.

Proposed Hybrid Model

Accordingly, the IPC would support a hybrid compliance model using ICANN Model 1 as a starting point, with the following additional proposed enhancements.

---

[2] ICANN has explicitly recognized the importance of bulk access to data to fulfill legitimate purposes. For example, with respect to zone data, ICANN has stated "one form of zone file access provides anticrime organizations, businesses, law enforcement and researchers with a means to download the entire zone file 'in bulk.' These organizations apply the bulk zone data in many ways, and among the most important of these applications are efforts to combat phishing, spam, brand and trademark infringements, and other malicious uses of domains." (emphasis added) See: https://czds.icann.org/en/help

[3] See self-certification criteria, *infra*.

1. **Inclusion of registrant email address in Public WHOIS**

We strongly urge that ICANN Model 1 be modified so that Registrant e-mail address is always included in Public WHOIS. For intellectual property rights enforcement efforts, as well as for a substantial number of law enforcement and other consumer protection efforts, the registrant's e-mail address is typically the most important data-point to have available. Moreover, an e-mail address is vital to fulfilling the stated purpose of "enabling a reliable mechanism for identifying and contacting the registrant." Providing only the registrant name and physical address in the Public WHOIS does not adequately fulfill that purpose. In IPC members' experience, registrant e-mail addresses included in WHOIS are far more likely to be accurate than the name and physical address data, which further highlights the importance of the e-mail address remaining publicly available. Finally, including the registrant's e-mail address will have only limited incremental impact on the privacy interests of registrants, particularly given that ICANN Model 1 already envisions publication of the registrant's physical address.

We also note that the decision to include the technical and administrative contacts' e-mail addresses in the public data for Model 1, but not the registrants' email addresses, appears arbitrary. All three e-mail addresses should be publicly available.

2. **True self-certification rather than case-by-case review**

With respect to tiered access for data not published in Public WHOIS as proposed in ICANN Model 1, we support such an approach based on true self-certification. Although ICANN Model 1 refers to "self-certification," the procedure could be read to require a review by the registry or registrar of every request for non-public WHOIS data submitted to it. This would be extremely burdensome on registries/registrars and users, and would result in substantial delays to accessing potentially time-critical data.

Instead, we strongly recommend that a true self-certification process be implemented, whereby the requestor certifies that it needs access to the data for one of the purposes set out in ICANN Model 1 (which include "intellectual property protection" – see page 6 of the Document), certifies that it will comply with GDPR when processing WHOIS data covered by the GDPR, and is given access automatically. The compliance model submitted by COA provides an example of a true self-certification process, which ICANN should strongly consider in implementing this element of the proposed hybrid solution.

Another alternative to the COA self-certification model could be based on ICANN org's suggestion, set forth in footnote 15 of the Document. The self-certification and approval process should be similar to and based on that currently used by registries to approve access to Zone File Data in the Centralized Zone Data Service (CZDS). Using that process as a basis, we suggest the following could provide another model for a true self-certification process:

Requirements for Self-Certification:

1. Name of Requestor
2. If Requestor is not an individual, name of individual completing self-certification on behalf of Requestor
3. Physical Address of Requestor
4. E-mail Address of Requestor
5. Phone number of Requestor
6. Purpose of Request (note: could be tick-box to select one of the 5 purposes set forth for ICANN proposed interim models)
7. Agreement, under penalty of perjury, to all of the following conditions (tick-box: yes/no):
    a. Is the requested data necessary to further the purpose set forth in item 6?
    b. Will the data requested be used for the potential establishment, exercise or defense of legal claims?
    c. Requestor will process data received in accordance with the purpose for which access is sought as indicated in (6.), above.
    d. Requestor will take all reasonable steps to protect against unauthorized access to, use of, or disclosure of received data.
    e. Requestor will comply with the GDPR and other applicable laws with respect to the received data.
    f. Requestor will not use received data to: (i) allow, enable or otherwise support any marketing activities to entities other than the user's existing customers, regardless of the medium used (such media include but are not limited to transmission by e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts of mass unsolicited, commercial advertising or solicitations to entities), (ii) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator or any ICANN-accredited registrar, or (iii) interrupt, disrupt or interfere in the normal business operations of any registrant, with the understanding that investigations into potential illegal or abusive activity of a registrant and efforts to stop such alleged illegal or abusive behavior through criminal or civil legal action or communication directly with registrant, registrar, Registry Operator or any other intermediary concerning such alleged illegal or abusive activity shall not be considered an interruption, disruption or interference in normal business operations of any registrant.

Registrar Response to Self-Certification:

If the requestor properly completes items 1-6 and affirms by ticking "yes" to items 7(a)-(f), then the registrar/registry must grant immediate access to the non-public data to the requestor.

This self-certification process should comply with the GDPR for a number of reasons. First, it limits use of the data by the requestor to a legitimate purpose and imposes obligations on the requestor to process and use the data in compliance with the GDPR and any other applicable

laws. Therefore, it embraces the principles relating to the processing of personal data as set forth in Article 5 of the GDPR. Second, because this self-certification affirms in item 7(b) that the requested data will potentially be used to establish, exercise or defend a legal claim (either civil or criminal), it serves to relieve the registrar of balancing the interests of the registrant and requestor with respect to the right to object set forth in Article 21 of the GDPR.

Whether a true self-certification process is adopted as proposed in the COA model or along the lines outlined above, it is critical to a functional system that the self-certification process and requirements be uniform across all gTLD registrars in order to ensure consistency and reliability.

We believe this proposed hybrid model is consistent with many elements of the community submitted models, including those submitted by COA, iThreat, AppDetex and Frederick Felman. As suggested by all of those models, public safety, law-enforcement and legitimate third-party interest (including IP rights holders) purposes need to be clearly identified and stated. Restrictions on public WHOIS should be limited to registrants and data collection/processing that fall explicitly within the scope of the GDPR. Consent from the registrant should be sought as a means of including personal data in public WHOIS. And finally a reasonable, reliable, consistent and expedited process must be put into place for legitimate third-party access to non-public data.

Comments on ICANN Model 2

Model 2 (both A and B) strays from the objective by extending beyond the application and requirements of the law (the GDPR) with which the model seeks to comply by: (i) unjustifiably applying the model to data not covered by the GDPR – the data of legal persons (in both A and B); (ii) applying the model to all registrations (in B) irrespective of the more limited application of the GDPR, and (iii) overly restricting the data elements that remain available in Public WHOIS.

We consider our suggested hybrid, using ICANN Model 1 as a starting point and enhanced with the suggestions outlined above, to be far preferable to ICANN Model 2, and more consistent with the objective. The following are the most important areas where ICANN Model 2 falls short:

1. A distinction must be drawn between registrants that are natural persons and those that are legal persons. The GDPR only protects personal data of "identifiable natural person[s]" and therefore legal persons are excluded from its scope (see Article 4(1) of GDPR).

2. As set forth in our comments above, it is critical that the Registrant e-mail address always be included in Public WHOIS, in addition to Registrant Name and Physical Address. In seeking advice from DPAs, we urge that the interim compliance model selected by ICANN ensures that Registrant e-mail address, Registrant Name, and Registrant physical address all be included in Public WHOIS.

3. At minimum, registrars and registries should be required to retain data two years beyond the life of the domain name registration (as provided for in ICANN Model 1).

A standardized accreditation/certification process with mutual recognition for third-party requestors as proposed in ICANN Model 2 would be desirable and potentially lessen the burden on registrars/registries and third-party requestors and provide greater certainty. If such a process were not ready in time, then ICANN should pursue a true self-certification process as suggested above.

Comments on ICANN Model 3

ICANN Model 3 falls far short of the objective and is seriously flawed. It would impose unnecessary and unacceptable burdens on contracted parties as well as third parties who rely on data access. By applying GDPR requirements to all registrations, regardless of natural or legal person status or geographic location of the registry/registrar or registrant (data subject), and then requiring the registrar to make a determination on its own on a data element-by-data element basis (other than thin WHOIS data) whether a particular element does or does not constitute personal data not only imposes unacceptable burdens and responsibilities on registrars, but also guarantees grave inconsistency and chaos in implementing a cohesive Public WHOIS system. Moreover, by permitting third parties with legitimate interests to access non-public data only pursuant to subpoena or court order, ICANN Model 3 does not even come close to fulfilling the statement of purposes that ICANN org itself has proposed, and goes far beyond the requirements of the GDPR. To that end, we note the advice from Hamilton law firm dated 21 December 2017 that a model requiring requestors to seek court orders "*would risk putting courts and other authorities under significant pressure if there was no easily accessible way to access relevant information other than requesting a judicial order.*" Because this model strays so far from the objective, does not meet the identified purposes, and imposes unacceptable burdens on numerous stakeholders, it should be rejected and not further considered.

Procedural Concerns

Finally, we must note our consternation with ICANN's process for addressing this critical matter. The issues and questions presented are complex and deserve careful consideration. The compressed deadlines imposed by ICANN org over the past two months have made that difficult. Moreover, ICANN org's initial intention to select a model two days following the deadline for submitting comments on the compliance models raised grave concerns that these and other comments from the community would not be given serious attention. ICANN has since stated that it is pushing back its decision-making deadline to mid-February; that said, while we are still concerned that this shift is merely to improve optics, we appreciate this reasonable accommodation and impress upon ICANN the need to use the extra time to duly and diligently review community input.

Respectfully submitted,

Intellectual Property Constituency