On 1/9/18, 07:59, "Amadeu Abril i Abril (CORE)" wrote:

Dear ICANN Team,

Please find below CORE Association's feedback on the "layered access" proposal made by the Hamilton law firm, as requested. CORE welcomes this opportunity, specially after so many years requesting, without any success, a global, systematic approach to WhoIs publication in light of EU legislation

As a summary, and prior to submitting our model for Whois compliance in the upcoming days, we would like making the following considerations:

1.While the GDPR changes the procedural, and compliance approach, and most notably the geographic and institutional scope of the EU Data protection legislation, it *DOES NOT* modify in any relevant extent the *substantive* requirements affecting Whois. New implementation, new enforcement, new legal consequences are at stake but not new substantive requirements. Past experiences and solutions approved by DPAs, therefore, hold their validity.

2. In this regard, we support Hamilton's claim that there are valid arguments in light of the GDPR (as before) for maintaining a public directory service (Whois), with the needed adjustments, as discussed below.

3. Where the Hamilton report fails to make a fundamental distinction, though, is that all the arguments relating to public directories (unrestricted access) deriving from Trademark or Commercial Registries do not derive from a generic "public interest to know", but to a more concrete public interest to protect consumers and trust in trade, perfectly defined in all EU Member States legislations, and by the EU itself. This public interest reasons relate to the legal, social consequences of carrying out *economic activities*, the consequences of "acting in trade". This is why the identity, and the contact details, of entities (and individuals) carrying out those activities are not prevented from publication, but, quite the contrary, are mandated to be published (on those special registries, but also on their websites and online communications). The analogy with real state (land property) registries is unfortunate: while owners of real state are publicly identified, for the same reasons above, the private domicile, telephone email of private individuals, as such, is not allowed without specific and free consent. And this is the *fundamental* flaw of current Whois implementation.

4. In this regard the WP29 letter from 2017-12-06 stresses that the *primary* concern to be addressed is that the "consent to publication as contractual requirement to obtain a domain name" is *clearly* an insufficient ground for publication when it refers to *individual* domain-name holders. Unless we grant them a real consent-granting (or refusing) mechanism, no publication will be acceptable.

5. As already implemented by some EU TLDs, both gTLD (.cat) and ccTLD (.fr) after extensive discussions with their respective DPAs, an *OPT-OUT* mechanism MUST be provided, at least for INDIVIDUALS not using their domain names for economic activities.

6. Even with such opt-out mechanism in place, and the distinction between individuals and legal

entities as registrants, some contact data, such as fax numbers, physical address for TechContact, etc. makes no sense in 2018, and should probably not be collected and processed anymore. And some personal data for corporate domain names should not be published, either. But this part exceeds the purpose of the feedback on layered access.

Therefore, our proposal on layered (or tiered) access is:

A) Provide a mandatory opt-out mechanism (at registration time, but also once a year with the Whois Data Accuracy Reminder) for, at least individual registrants. Perhaps extended to personal contact data (individual 's names, phones, emails) for all domain names.

B) As for CONTACTING the registrant, Registries should have an online form available to third parties, which would be sent to registrants (but without disclosure of personal/contact information). This first step would mean access without disclosure.

C) INDIVIDUAL, ON REQUEST DISCLOSURE: law enforcement agencies should have access to registrant's data upon request. Bulk, unlimited access does not seem necessary, and in our experience, has not be requested by law enforcement.

Access for private legal issues, intellectual property and other, should be granted with certain conditions, including statement of purpose, and notification to registrant of such request.

We firmly believe that the issue will not be solved while we keep treating the name of the registrant for "google.com[google.com]" in the exact same way as the personal phone number of an individual running a personal blog on her own domain name. One size does not fit all. And beyond the question of legitimate purpose, the free and unequivocal consent is the key to maintaining some data publicly available, while the rest should be treated under a layered access approach.

Amadeu Abril i Abril
Chief Policy Advisor
CORE Association