From: Dean Marks
Sent: Thursday, 31 October 2019
To: Maarten Botterman; Leon Sanchez

Subject: Congratulations and Request

Dear Maarten and Leon,

Congratulations on your recent election to Chair and Vice Chair of the ICANN Board of Directors. I along with all the COA members are looking forward to your leadership and to working with you.

I am writing to raise the issue of the ongoing unilateral hold that ICANN org has placed on the implementation of the Privacy/Proxy Services Accreditation Issues Consensus Policy ("PPSAI Consensus Policy") that was unanimously approved by the Board in 2016. As you aware, ICANN org has taken the position that there are important and overlapping issues to Privacy & Proxy Service Accreditation being analyzed within the context of the EPDP that warrant keeping the PPSAI Consensus Policy on hold. We disagree for the following reasons:

1. The EPDP will not address access to registrant data that is masked by privacy/proxy services. An increasing amount of registrant data, however, is masked by such services. That is making investigations by both law enforcement and by parties with legitimate interests (such as IP rightsholders) of illicit online activity more difficult. See for example, the following two recent articles: https://www.csoonline.com/article/3443049/cobalt-cybercrime-group-might-be-launching-magecart-skimming-attacks.html [csoonline.com] and http://www.circleid.com/posts/20191023_cybercriminals_benefiting_from_stalled_privacy_proxy_policy/ [circleid.com]

2. The Disclosure Framework set out in the PPSAI Consensus Policy is consistent with the accreditation and authentication Key Concepts of the Unified Access Model for gTLD Registration Data as set forth in the paper dated October 25, 2019 ("UAM Paper") that ICANN submitted to the European Data Protection Board. Because: (i) the PPSAI Consensus Policy has already been fleshed out, adopted by the multistakeholder community and unanimously approved by both the GNSO Council and the Board, and (ii) is consistent with the approach being proposed for access to registration data that is not masked by such privacy/proxy services (but is redacted in accordance with the Specifications implemented to comply with the GDPR), moving forward with the implementation of the PPSAI Consensus Policy should both help inform/support the work of the EPDP and complement it.

We think the work undertaken by ICANN org in putting together the UAM Paper and submitting it to the European Data Protection Board is substantively valuable and useful in supporting the efforts of the EPDP team. We firmly believe that taking the hold off the implementation of the PPSAI Consensus Policy and moving it forward will serve to provide additional insights and support for the work of the EPDP. Perhaps even more importantly, it will address an entire area of access to registration data, which ICANN org has explicitly recognized in the UAM Paper as serving the public interest, that will neither be addressed nor solved by the successful conclusion of the EPDP Phase 2 work. Finally, we respectfully submit that the Board should question whether the continued unilateral block imposed by ICANN org on policy that was successfully developed and approved by the ICANN multistakeholder community (and the Board itself) undermines the trust and adherence to fundamental principles and foundations of the multistakeholder model.

Please find attached to this email a short paper prepared by Steven Metalitz, who served as Co-Chair of the PPSAI Working Group. It explores these issues in greater depth and gives a substantive summary of the critical elements of the Disclosure Framework of the PPSAI Consensus Policy.

We would like to meet with you during the upcoming meeting in Montreal to discuss this issue if possible and will be happy to meet early in the morning or late in the evening at your convenience--or any other time--given that we appreciate that your schedule during the day is full.

Many thanks for your consideration.

Best regards,
Dean

Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability ("COA")

PRIVACY/PROXY ACCREDITATION CONSENSUS POLICY:

CONNECTION TO PROGRESS ON THE EPDP AND THE NEED FOR IMPLEMENTATION

INTRODUCTION

On August 9, 2016, the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN) gave its unanimous approval to a consensus policy on accreditation of privacy and proxy services. ("PPSAI Consensus Policy") https://www.icann.org/resources/board-material/resolutions-2016-08-09-en#2.e This policy set standards for the accreditation of these services, whose purpose is to mask from public disclosure the contact information on domain name registrants that would otherwise have been made available via the then-current registration data service (WHOIS). Once fully implemented, the PPSAI Consensus Policy would prohibit ICANN-accredited domain name registrars from knowingly accepting domain name registrations from unaccredited privacy/proxy services.[1] Although the work of the Implementation Review Team ("IRT") on this consensus policy was nearly completed in 2018, ICANN Org put a unilateral hold on the work of the IRT and continues to do so.[2]

Among many other features of the accreditation system created by the PPSAI Consensus Policy, these services were obligated to adhere to a Disclosure Framework governing requests from intellectual property holders for disclosure of registrant contact data that would otherwise be masked by the service. This Disclosure Framework was the result of two years of intensive negotiations among all relevant constituencies (including privacy advocates and European-based registrars), in full cognizance of the then-applicable European Data Protection Directive. It provides a concrete example of a good faith effort to define the circumstances and procedures under which a data requester's legitimate and compelling need for access to registration data could be balanced against the legitimate privacy interests of the data subject (the privacy/proxy service's customer, i.e., the actual domain name registrant). As such, the compatibility of this ICANN consensus policy with the current European data protection regime (as embodied in the General Data Protection Regulation, or GDPR) is an important issue for current consideration, and should be pursued simultaneously and in conjunction with ICANN's efforts to establish a unified access mechanism/model for registration data overall in the current GDPR environment. [3]

---

[1] As defined in the PPSAI Consensus Policy, the main difference, for data access purposes, between a privacy service and proxy service is that the former displays in WHOIS the name of the actual registrant, along with substituted contact information, while the latter substitutes the contact information of the service provider in toto for that of the beneficial registrant in the WHOIS output. The working group report provides that "privacy and proxy services are to be treated the same way for purposes of the accreditation process." Final Report, at 8.

[2] See: https://www.icann.org/en/system/files/correspondence/namazi-to-drazek-et-al-05sep19-en.pdf

[3] In ICANN org's document, dated October 25, 2019 submitted to the European Data Protection Board to seek guidance on a potential Unified Access Model for gTLD Registration Data, ICANN org notes that "[t]he implementation of this [PPSAI Consensus Policy] accreditation program is currently on hold, pending completion of EPDP Phase 2." See footnote 6 of the guidance request: https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf

It is clear that the EPDP will not be addressing registration data that is masked by a privacy or proxy service. According to a recent article in Circle ID, "Today, nearly 50 million registered domains (and growing) use privacy/proxy services. Providers of these services create obstacles to access domain name owner information, even when formally requested by parties with clear-cut examples of how the domain name is being used for abuse and malicious behavior. ICANN's continued inaction is hurting mitigation efforts and making a bad situation worse."[4]

Given that the PPSAI Consensus Policy: (i) contains a concrete disclosure framework that not only has been fully approved by the ICANN multistakeholder community and the ICANN Board, but also is consistent with what is being proposed for a Unified Access Model for gTLD data that is not hidden by such privacy/proxy services, and (ii) addresses critical registration data disclosure issues that will not be resolved by the EPDP, the PPSAI Consensus Policy should be taken off hold and pursued in conjunction with the work of the EPDP.

THE PRIVACY/PROXY ACCREDITATION SYSTEM AND THE DISCLOSURE FRAMEWORK – OVERVIEW

The most authoritative source of information regarding the privacy/proxy service accreditation policy adopted by the ICANN Board in the PPSAI Consensus Policy can be found in the Final Report on the Privacy & Proxy Services Accreditation Issues (PPSAI) Policy Development Process, issued in December 2015. https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf ("Final Report"). This report was the work product of a working group (WG), convened in 2013 in accordance with ICANN's long-standing multi-stakeholder policy development framework, that comprised representatives and active participants from all relevant ICANN constituencies, including ICANN-accredited registrars[5] and registries; business and intellectual property interests; civil society groups represented in ICANN's Noncommercial Users Constituency (including several vigorous privacy advocates); and governmental and law enforcement representatives (via ICANN's Governmental Advisory Committee). The rest of this memo summarizes key elements of the Final Report, but the full report text should be consulted for details.

While many aspects of the policy recommended by the WG, and ultimately approved unanimously by the ICANN Board, implicate issues of relevance to GDPR compatibility,[6] this memo focuses on the issue of disclosure, defined in the WG report to mean revelation of "the identity and/or contact details of the privacy/proxy service customer to a third party requester."[7] The PPSAI Consensus Policy includes a number of procedural or transparency requirements regarding the disclosure policies that services would have to meet in order to achieve and maintain accreditation with ICANN. For example, service providers would be required to include on their websites a link to a request form that third parties could

[4] See: http://www.circleid.com/posts/20191023_cybercriminals_benefiting_from_stalled_privacy_proxy_policy/
[5] Throughout the development of the consensus policy, virtually all existing privacy/proxy services were operated by ICANN-accredited domain name registrars, usually through wholly owned subsidiaries or other corporate alter egos. Thus, the registrars represented the interests of the privacy/proxy service providers.
[6] See, e.g., provisions regarding validation and verification of the accuracy of information regarding domain name registrants who choose to employ privacy/proxy services. See Final Report at 9, 53-54.
[7] Final Report at 8. In the policy, Disclosure is to be distinguished from Publication, in which the customer's contact details would be published in the publicly accessible WHOIS system. Id. at 7.

use to make disclosure requests, and to publish in their publicly available terms of service "the specific grounds upon which a customer's details may be Disclosed or Published." [8]

The PPSAI Consensus Policy did not contain generally applicable substantive provisions defining the circumstances under which disclosure of customer contact data to a requesting third party would be mandated or could be refused.[9] However, it did include an "Illustrative Disclosure Framework" setting forth procedures and standards that accredited service providers would be required to follow for one category of requests: those made by or on behalf of intellectual property rights holders who claim "that registration or use of a domain name for which the Provider provides privacy/proxy services infringes copyright or trademark rights of the requester." [10] This Disclosure Framework --- labeled Illustrative because it covered only one category of third-party requests (although it could readily provide a template or starting point for the development of similar frameworks regarding other types of requests) --- can be found in Annex B of the Final Report. [11]

The preamble to the Illustrative Disclosure Framework sets forth its goals, clearly reflecting a balance of the key interests:

By facilitating direct communication among Requesters, Providers, and Customers, this policy serves the public interest and seeks to balance the interests of concerned parties. It aims to give Requesters a higher degree of certainty and predictability as to if, when, and how they can obtain disclosure; to give Providers flexibility and discretion to act on requests for disclosure and not require that disclosure automatically follow any given request; and to include reasonable safeguards and procedures to protect the legitimate interests and legal rights of Customers of Providers. [12]

DISCLOSURE FRAMEWORK: KEY FEATURES

The ICANN-approved Illustrative Disclosure Framework spells out in detail:

- how requests by intellectual property rights holders for disclosure of WHOIS data should be handled;
- what such requests must contain; and
- permissible and impermissible grounds for rejecting such requests.[13]

Disclosure Framework Section I: Provider Process for Intake of Requests[14]

The Framework requires privacy/proxy service providers to establish a point of contact for electronic submission of disclosure requests by intellectual property rights holders. Providers are permitted

[8] Final Report at 10.
[9] See Final Report at 47.
[10] Final Report at 47, 83 (Annex B).
[11] Final Report at 85-93.
[12] Disclosure Framework (Annex B to Final Report) at 85.
[13] The Disclosure Framework also addresses, to a lesser extent, review of decisions by service providers granting or denying disclosure requests.

[14] Disclosure Framework at 85-86.

(though not required) to implement safeguards against abuse of the submission process, such as requiring requesters to register themselves or their organizations; requiring log-in credentials or similar authentication mechanisms; imposing "a nominal cost-recovery fee for processing submissions"; and revoking access to the submissions process for "egregious abuse of the [request submission] tool or system." The Framework also authorizes service providers to pre-qualify "trusted requesters" whose complaints could follow a more streamlined process. **Many of these elements are similar to the Key Concepts outlined in ICANN Org's recent document submitted to the European Data Protection Board entitled "Exploring a Unified Access Model for gTLD Registration Data" dated 25 October 2019**. See in particular Section 3 at page 10 at: https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf. .

Disclosure Framework Section II: Request Templates for Disclosure [15]

This lengthy section of the Framework sets the minimum criteria that requesters must meet to successfully invoke the disclosure request process. It includes three largely parallel sets of evidence to be submitted, depending on whether the complaint arises from alleged trademark infringement in the registration of the domain name itself (e.g., cybersquatting); or whether the complaint is that the registrant is using the domain name either to infringe a copyright (e.g., to resolve to a site enabling copyright piracy) or to infringe a trademark (e.g., to resolve to a site making counterfeit goods available). In each case, the key minimum requirements are:

- Specificity: The requester must identify the domain name involved (or the URL where infringing activity is taking place); the trademark or copyright work alleged to be infringed; and information about how the claim of a valid trademark or copyright can be verified;
- Identity and full contact information of the requester (including, where applicable, attestation of authority to act on behalf of the rights holder);
- Attestation of good faith and reasonable basis: The requester must provide, under penalty of perjury or equivalent sworn statement, "verifiable evidence" that "provides a basis for reasonably believing" that an infringement is occurring and is not subject to an overriding defense;
- Use limitations and submission to jurisdiction: The requester must certify that it will use the requested data only in accordance with applicable data protection laws, and only for intellectual property rights enforcement purposes, and that it will submit to jurisdiction in its home country, and in a jurisdiction specified in the provider's request form, for adjudication of allegations of misuse (either by using the disclosed information for non-enforcement purposes , or by obtaining the requested data through knowingly false statements). [16]

These request templates, while tailored for the intellectual property infringement environment, provide a starting point that could be elaborated to cover requests for disclosure of registrant identity and contact data from a broader range of third-party requesters with legitimate interests.

[15] Disclosure Framework at 86-90.

[16] A brief Annex to the Disclosure Framework provides definitions for wrongful disclosure and misuse of disclosed information, and specifies that nothing in the Framework precludes any party from seeking other available remedies at law. Disclosure Framework at 93.

Disclosure Framework Section III: Provider Action on Request

This section of the Illustrative Disclosure Framework spells out, in concrete terms, the range of options for service provider action in response to a disclosure request. As noted in the Framework's preamble quoted above, the goal is to balance the interests of requesters (predictability and certainty); service providers (flexibility and discretion); and service customers (including legitimate privacy interests). **Of particular relevance in the GDPR environment, the Framework provides a mechanism for recognizing the specific legitimate interest being pursued by the requester and for determining whether, in an individual case, that interest would be overridden by the interests or fundamental rights of the domain name registrant (i.e., the customer of the privacy/proxy service provider).** [17]

Procedurally, this section of the Framework requires the service provider to notify its customer of disclosure requests and to ask for a response (including any reasons for objecting to the request) within 15 days. The provider must respond to the request within a defined time period after receiving the customer's response (or the expiration of the 15 days), either disclosing the requested data or giving specific reasons for refusing to disclose.[18]

The Framework then lists seven permissible reasons for "reasonably refusing" disclosure, followed by five reasons upon which the provider may not permissibly rely to refuse disclosure.[19]

The list for "reasonably refusing" disclosure covers three main types of cases:

- where the evidence presented (including any information provided by the customer or developed by the provider) falls short of meeting the "verifiable evidence of wrongdoing" standard set forth in the request submission templates;[20]
- where there is specific information, facts or circumstances showing that the alleged intellectual property infringement is a pretext for seeking disclosure, or that disclosure would endanger the safety of the customer;[21]
- where the request is in effect moot because the requested data has already been published in WHOIS, or because the customer has taken advantage of an (optional) service provider policy to surrender the registration rather than consenting to disclosure. [22]

The list of reasons for which the provider may <u>not</u> rely upon to refuse disclosure include:

- the absence of a court order or subpoena;
- that a civil action, UDRP or URS proceeding, is not pending or hasn't commenced;
- the fact that the intellectual property violation being alleged is embodied in content on a website associated with the domain name, rather than in the domain name itself. [23]

[17] See GDPR Art. 6.1.f.
[18] The Framework provides for an extension of these time frames in "exceptional circumstances." Disclosure Framework at 91, section III.B.
[19] Disclosure Framework sections III.C and III.D, at 91-92.
[20] Disclosure Framework sections III.C.ii ,iii and vii, at 91.
[21] Disclosure Framework sections III.C.v. and vi, at 91.
[22] Disclosure Framework sections III.C.i and iv, at 91.
[23] Disclosure Framework section III.D, at 92.

Finally, this section of the framework requires providers to "accept and give due consideration" to requests to reconsider any refusal to disclose. [24]

Taken as a whole, section III of the Disclosure Framework clearly represents a refined and well-articulated process to apply, in the specific setting of intellectual property complaints, the calculus set forth in Art. 6.1.f of the GDPR. That is whether a legitimate third party interest to justify disclosure has been presented and, if so, whether interests or fundamental rights and freedoms of the proxy/privacy service customer (who, if a natural person, qualifies as a data subject) are sufficient to override that legitimate third party interest. This is not surprising, even though the issuance of the Final Report predates by a few months the publication of the GDPR. The calculus set forth in Art. 6.1.f of GDPR is virtually identical to that enshrined in Article 7(f) of the Data Protection Framework Directive of 1995, with which many working group participants were intimately familiar (and under which many of the European-based business and registrar interests represented on the Working Group had operated for many years).

CONCLUSION

ICANN org has correctly noted that "Domain name registration data is a critical tool for identifying the actors behind domain names. . . . Access to registration data, commonly known as WHOIS data, serves the public interest and contributes to the security and stability of the Internet by providing contact information to support efforts related to consumer protection, cybercrime investigation, DNS abuse, and intellectual property, and to address appropriate law enforcement needs."[25] With so much domain name registration data being masked by privacy/proxy services, a disclosure framework such as developed in the PPSAI Consensus Policy should be implemented at least contemporaneously with addressing the general issue of legitimate access to registration data that is redacted in response to the GDPR (and that is not masked by such privacy/proxy services). **Far from detracting from the work of the EPDP, moving forward with the implementation of the PPSAI Consensus Policy should assist in supporting and informing the work of the EPDP. Furthermore, it will serve the public interest goal correctly articulated by ICANN org of ensuring legitimate access to registration data when such privacy/proxy services are used to mask the data.**

[24] Disclosure Framework section III.E, at 92.

[25] See: https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf at page 4.