MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

Brian J. King
Director of Internet Policy and Industry Affairs
E: Brian.King@markmonitor.com
T: +1(443) 761 3726
markmonitor.com
clarivate.com

August 2, 2018

Göran Marby
President and & CEO
ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Dear Göran,

As noted in the SSAC Advisory Regarding Access to Domain Name Registration Data ("SAC101")[1] and the GAC's Panama Communique[2], access to WHOIS information is vital to ensuring the security and stability of the Internet, yet access to WHOIS data has become unreliable due to disparate implementations of the European Union's General Data Privacy Regulation and ambiguity in the Temporary Specification for gTLD Registration Data[3] approved by the ICANN Board on May 17th. Accordingly, MarkMonitor is pleased to have the opportunity to comment and provide feedback on several of the questions and statements presented in proposed Unified Access Model ("UAM").

Most importantly, MarkMonitor urges ICANN to support the inclusion, in any final model, of the work already undertaken by members of multiple and various stakeholder groups, to develop and draft the Accreditation & Access Model ("AAM")[4] currently on version 1.7. We believe the collaborative efforts being made by the drafters of AAM should continue with ICANN's full encouragement and that any final accreditation and access model contain several key elements of this model that have been carefully thought out and proposed.

More specific comments on the UAM follow:

Questions 1 & 2: Who would be eligible for continued access for WHOIS data via the Unified Access Model? Who would determine eligibility?

MarkMonitor supports the extensive list of proposed eligible entity types and examples outlined in the AAM.

---

[1] https://www.icann.org/en/system/files/files/sac-101-en.pdf
[2] https://gac.icann.org/contentMigrated/icann62-panama-communique
[3] https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf
[4] https://www.icann.org/en/system/files/files/draft-whois-accreditation-access-model-v1.7-23jul18-en.pdf

The UAM requests significant contribution from European Economic Area ("EEA") country GAC members and guidance from these governments and other GAC members with experience in data privacy-related policymaking is essential. Accordingly, ICANN should accept and follow the GAC Advice from the Panama Communique, as well as SAC101, and act promptly to ensure certainty of full WHOIS access for the legitimate purposes defined by these bodies.

Article 6, Section 1(e) and (f)
ICANN should follow the SSAC Advisory and GAC Advice, and should formally acknowledge that access to full WHOIS data is legitimate for the purposes of "law enforcement; cybersecurity; consumer protection and the protection of intellectual property"[5] and that these legitimate purposes are not overridden by the interests or fundamental rights of relevant data subjects[6] who choose to avail themselves of the DNS. Because reliable WHOIS information is key to the openness, interoperability, resilience, security and stability of the DNS, the privacy interests of informed domain name registrants who seek to avail themselves of the power of the global DNS should not override the legitimate interests of WHOIS requestors that self-certify as law enforcement, cybersecurity, consumers, or intellectual property rights enforcers, and agree to a sufficient Code of Conduct around their use of the data. We encourage ICANN to help lead the community toward clearly defining the legitimate interests for requesting WHOIS data under the regulation.

In addition to considering subsection (f) as the applicable law, ICANN should marshal the appropriate legal advice to justify WHOIS data being lawfully processed as it is "necessary for the performance of a task carried out in the public interest," "in the exercise of official authority vested in the controller," or both, including in such a scenario where ICANN is the controller in an RDAP setting and ICANN is processing the data in its official authority to coordinate the DNS and/or to perform its task in the public interest.[7] While the threshold for processing on public interest grounds may be high, ICANN's role as the coordinator of the global DNS for the public interest should meet this high threshold. ICANN should consider whether it already has, or needs to act to secure, "official authority" for the purposes of subsection (e).[8]

Establishing lawfulness by either of these two bases in subsection (e) could eliminate the need for the language "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" from subsection (f) and passed through problematically in the Temporary Specification. This language has failed legitimate users, as it

---

[5] https://gac.icann.org/contentMigrated/icann62-panama-communique
[6] GDPR Art 6 Sec 1(f) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en
[7] GDPR Art 6 Sec 1(e) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en
[8] Id.

has proven to be too nebulous to be useful *per se* to the registrar community, especially when more than 2,400 accredited registrars each perform their own balancing test for each request received. Many registrars do not have the bandwidth to do so, and all registrars are now being asked, unfairly, to perform this balancing test in a way that gives sufficient credence to the legitimacy of overriding interests, while facing the crippling fines possible under GDPR if we get it wrong. If ICANN must rely on subsection (f), it should amend the Temporary Specification to clarify that the balancing test should be performed as articulated in the Article 29 Working Party's guidance[9], and that, absent an articulated overriding interest, access should be granted to requestors who have legitimate interests and who agree to appropriate safeguards.

ICANN should also request legal advice that confirms that subsection (f) does not apply to ICANN as a "public authority", a term potentially applicable to ICANN as it is used broadly throughout the GDPR's text but not explicitly defined.[10]

Other Legal Bases for Processing

MarkMonitor encourages ICANN to have stakeholders identify legal bases for lawfully processing WHOIS data under Preamble 49 ("ensuring network and information security").

ICANN should also request stakeholders define who can process WHOIS data lawfully under Preamble 122 for ("private bodies acting in the public interest").

ICANN must establish lawful processing under a "non-subsection (f)" provision and/or provide greater certainty of access where legitimate interests override data privacy interests. ICANN is aware that including the subjective overriding interest language in the Temporary Specification obviates any real compliance obligation for contracted parties to provide non-public WHOIS information, even to those requestors with legitimate interests, if the contracted party merely states that the data subject's interests override. Either by amending the Temporary Specification, or preferably by securing endorsement from the Data Privacy Board, ICANN must not delay in addressing this, even for the pendency of the EPDP. Leaving a compliance loophole would be inconsistent with GAC Advice and SSAC Advisory.

Question 3: How would authentication requirements for legitimate users be developed?

We understand that ICANN is looking for legal justification to select a "body which has an appropriate level of expertise", and Europol may have sufficient expertise with a legal basis

[9] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[10] Id.

under the GDPR. Interpol, which already coordinates law enforcement on a global scale, may also have sufficient expertise to accredit global law enforcement agencies.

Both WIPO and the TMCH are fine examples of bodies that could accredit IP rights holders. ICANN could also consider USPTO, OHIM, and digital certificate providers as bodies with sufficient expertise to accredit legitimate users. ICANN should consider whether one Authenticating Body should be selected to accredit all remaining (non-law enforcement) Eligible User Groups, or whether specialized knowledge is required and ICANN should contract specific Authenticating Bodies for each Eligible User Group (e.g. WIPO for parties with legitimate purposes under IP protection grounds and ISC2 for parties with legitimate purposes under information security grounds, vs. having Deloitte, for example, accredit all parties accessing data for non-LEA purposes). In any event, this service should be put out to bid as soon as possible to ensure timely selection and ramp up.

Question 5: What would be the overall process for authenticating legitimate users for access non-public WHOIS data under the Unified Access Model?

We should strive for the least technically onerous solution possible to minimize the implementation burden on contracted parties. The Authenticating Body should be able to provide the credential to the authorized user without involving a third-party "credential provider," and we would not object if Authenticating Bodies found it prudent to involve such a provider. In any event, the registrar or registry operator should be able to rely on a properly-authenticated requestor, and should not be required to validate the request further. Authenticating Bodies should develop their own authentication processes, subject to community input and regular review, audit, and improvement from the community.

Question 6: What scope of data would be available to authenticated users?

With an understanding of GDPR's data minimalization principle, we acknowledge that different legitimate purposes may require different levels of access to the non-public WHOIS data fields. Practically, we submit that this process must be workable for contracted parties, and must not be unduly onerous.

Question 7: Would registry operators and registrars be required to provide access to non-public WHOIS data to all authenticated users?

Yes.

Question 8: Would the Unified Access Model incorporate transparency requirements?

Yes, so long as the software engineering required to implement the logging requirements are not unduly burdensome on contracted parties. This will be a serious concern for many contracted parties, including MarkMonitor. We submit that building different logging mechanisms or logging exception mechanisms to accommodate or exempt sealed court order requests would be unduly burdensome.

Question 9: Would there be any fees as part of the Unified Access Model?

MarkMonitor would welcome the legitimacy, reliability, and contract certainty that we would expect from a fee-based access model, which fees are reasonably modest and serve a stated purpose of compensating Authentication Bodies and contracted parties for their efforts in supporting compliant, legitimate access. However, we would also caution ICANN against such a model as it could introduce financial incentives that might cause doubts about the impartiality of legitimate interest determinations. This would create an opposite end of the same risk/reward spectrum as the aforementioned current incentive to err by denying legitimate access.

Question 10: Would there be a process to review the effectiveness of the Unified Access Model?

Yes, we anticipate regular reviews and audits and any improvements to the model would be expected.

Question 15: Would there be multiple Codes of Conduct?

The best approach might be the simplest. We would like to understand what safeguards ICANN considers that might apply to some Eligible User Groups but not others. Pending further discussion on this, we currently submit that there should be one Code of Conduct for all eligible entities.

Question 16: How would the Codes of Conduct be developed?

ICANN should consult with the EU Data Protection Board and the GAC, and the ICANN community should develop these Codes of Conduct with consensus through the EPDP.

Questions: 18 & 19: What mechanism would be used to require compliance with the Codes of Conduct? Who would monitor and enforce compliance with the Code of Conduct?

MarkMonitor supports the contractual agreement and self-certification mechanism for requiring compliance described in the Unified Access Model. It's unclear how Authenticating

Bodies would be able to monitor for compliance with the Code of Conduct, so their role should be limited to responding to complaints of noncompliance with the Code of Conduct. ICANN Contractual Compliance should continue to handle registry operators' and registrars' adherence to contractual obligations.

Thank you for your consideration, and please do not hesitate to contact me to discuss this further.

Kind regards,

Brian J. King
Director of Internet Policy and Industry Affairs