MarkMonitor
*Protecting brands in the digital world*

Clarivate Analytics

**MARKMONITOR COMMENT ON THE COMMUNITY'S, AND ICANN'S, PROPOSED INTERIM MODELS FOR WHOIS COMPLIANCE UNDER THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR)**

## Introduction

MarkMonitor, part of Clarivate Analytics, appreciates the opportunity to comment and offer feedback to ICANN on the five interim models for WHOIS compliance that have been proposed by various ICANN community members and the three interim models proposed by the ICANN organization.

Since its founding in 1999, MarkMonitor has offered domain name management and brand protection services to hundreds of the leading and most recognized companies and consumer brands in the world. Access to, and use of, domain registration data through WHOIS is an important element of the domain management, anti-counterfeit, anti-piracy, and fraud services that MarkMonitor provides to its valued clients. In 2017, MarkMonitor used WHOIS records to send 46,000 email enforcements to domain registrants who were infringing our clients' trademarks or counterfeiting their brands. In addition, MarkMonitor used WHOIS data to complete more than 80,000 inbound domain name transfers. For its fraud work, MarkMonitor used WHOIS records to send 184,000 enforcement notices to registrars and registries. The use of WHOIS data to take down infringing domains and fake websites doesn't just benefit MarkMonitor clients, this work helps erode funding for organized crime, terrorism and sex trafficking, as well as enhances consumers' overall trust and safety in the Internet.

## Five Important Characteristics of a Model

Due to the importance of its ongoing counter-crime, anti-abuse and consumer protection efforts, MarkMonitor agrees with ICANN's statement that an interim model must "***ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible***."

With this vital goal in mind, MarkMonitor believes that the optimal WHOIS model should have, at minimum, these five important characteristics:

1) The model must not extend beyond the legal requirements of GDPR or apply to data not within the scope of the regulation;
2) The model must be easy for registrars and registries to implement with little financial cost or time delay;
3) The model must not increase a registrar or registry's risk for legal liability;

4) Third parties that have a legitimate interest or purpose for gaining access to non-public WHOIS data, must be allowed such access under the model; and
5) The model must not create unnecessary or costly legal processes or impediments to access the non-public WHOIS data.

These five important characteristics are evident, mostly, in ICANN's proposed Models 1 and 2 which have included many thoughtful elements from the Community Models (CM) #1 (iThreat), CM#2 (COA), CM#3 (ECO), CM#4 (proposed by Fred Felman) and CM#5 (Appdetex) proposed by various community members. ICANN's Model 3, however, contains elements that go far beyond the scope of the regulation and imposes new stringent, unnecessary and therefore unacceptable burdens on registrars and third party requestors. For these reasons, ICANN Model 3 should be immediately rejected and not considered for selection by ICANN or any community member. A model that reflects the framework of ICANN's proposed Model 1 would come the closest to meeting the objectives outlined above. We elaborate further on the reasons for this in the discussion and analysis below, and also point out the positive elements of Model 2.

**Discussion and Analysis**

In Community Models #1, #2, #4, and #5 and ICANN Model 1, a clear distinction is made between data belonging to a natural person and data belonging to a legal entity. GDPR was written to harmonize data privacy laws across Europe. Because GDPR applies only to data belonging to natural persons, these two models do not extend beyond the scope of the European regulation. ICANN Model 1 calls for the registrant to identify itself as a natural person or legal entity. CM#3 (ECO) and ICANN Model 2, however, do not contemplate creating a process for distinguishing between natural persons and a legal entity – a critical distinction under the regulation (See Article 4(1) of GDPR). Any adopted model should take this issue into account and a process created so that the domain name industry doesn't expand the intended scope of GDPR.

Under ICANN Model 1, most of the current WHOIS data is collected and displayed. As registries and registrars currently collect this information, these models keep WHOIS more or less intact except for the masking of registrant email contact.[1] This model follows ICANN's stated intention to preserve the existing WHOIS to the greatest extent possible. Few burdens are imposed by registrars or registries under these models because they resemble the current systems. The ECO Model suggests that much of the WHOIS data, historically collected, is not needed for the provisioning of domains and therefore creates risk to registrars. While it is true that registrars have been passing only "thin" WHOIS data on .COM and .NET to Verisign for

[1] While the CM#2 (COA) provides for masking of the registrant's name and email subject to access upon self-certification, it was submitted prior to Hamilton's 3rd legal memo, which acknowledged the viability of making the registrant's name and physical address publicly available. CM#2's (COA) strong preference is for a model that provides for registrants name, physical address as well as email address, publicly available.

decades, it is *critical that the full "thick" WHOIS data still be collected*, transferred to the registries, and be available to Internet users, cybersecurity professionals and law enforcement officials under prescribed circumstances. MarkMonitor fully supports making "thin" WHOIS data publicly available under any new model but also would like registrant email address to be included in the publicly seen data. In this era, contacting individuals via email address is the preferred and most used form of communication, even more than telephone communication or texting. MarkMonitor may be willing to support, however, proposed webform access or listing an anonymized email address as proposed in the CM#3 (ECO) Model.

Both CM#3 (ECO) and ICANN Model 2 opt for less public availability of data in favor of lowering the risk of legal liability to a registrar or registry because, under this model, those seeking access to non-public WHOIS data must certify to a centralized validation authority that they have a legitimate purpose for accessing the data. The GDPR allows for the disclosure to third parties based on a legitimate interest of private stakeholders. (See Art. 6(1)). A detailed certification and validation process relieves registrars from the burden of balancing the requestor and the registrant's interests on a case-by-case basis. SSL Certificate providers already do a reasonable simple form of validation for OV and EV SSL certificates. Some believe it could take more than four months to implement a centralized validation process, but MarkMonitor does not believe that is necessarily so. There are many existing cloud-based technologies, based on agile software and database development, that can do verification and validation services. These can likely be employed within four months. However if not, the community should look at the CM#2 (COA) Model and ICANN Model 1 which propose a self-certification process. Currently, access to registry zones files are requested through a self-certification process. While this process has admittedly created headaches for registries, an improved, more automated and stringent process could be developed for validating third party requestors. A robust self-certification process could be a stopgap measure until a centralized authority can be instituted.

Finally, none of the models proposed, with the exception of ICANN Model 3, impose any unnecessary legal burdens, heavy financial costs, or impediments on the third party requestors and registrars and registries due to having to obtain and process subpoenas, court orders, and injunctions. For the reasons mentioned previously, ICANN Model 3 should be rejected entirely.

**What The ICANN Models Lack**

Despite the promising characteristics of many of the community models and ICANN Models 1 and 2, there are two critical aspects of GDPR and WHOIS that are not adequately addressed by any model and therefore should be incorporated into any final proposed model to the community.

First, the ICANN models each fail to address bulk WHOIS access to the data which is especially useful to MarkMonitor brand enforcement efforts. Currently, registrars "whitelist" or grant access to their bulk WHOIS data to law enforcement and IP protection services who need WHOIS to do reverse WHOIS lookups or to investigate abuse by previously identified bad actors. ICANN must include access to bulk WHOIS in the final compliance model. MarkMonitor strongly encourages ICANN to maintain the contractual requirement that registrars offer bulk WHOIS access through port 43.

Second, the ICANN models do not sufficiently address the impact of data latency likely to be introduced through any new certification or validation schemes. Delays in accessing data could have substantial impacts on threat protection and security efforts and could also substantially slow down necessary checks. MarkMonitor believe any solution to certifying third party requestors for non-public WHOIS data should not introduce delays and there should be permanent access to WHOIS data on a query basis once a third party requester is accredited

**A Word About This Process**

MarkMonitor appreciates the fact that ICANN is soliciting feedback and comments from the stakeholders in the ICANN community, however, the opportunity has arrived far too late. Because of the delay, registrars and registries have already begun implementing their own WHOIS models based upon legal advice that they have each obtained. This will ensure that the community, law enforcement officials, trademark lawyers, consumers, and brand protection companies will now likely face a patchwork of differing models they will need to learn how to navigate and access.

MarkMonitor is also concerned that ICANN failed to consider the application of the current adopted procedure for resolving WHOIS conflicts with local privacy law. That process seemed to have been triggered by the letter from the Dutch Data Protection Authorities in November yet this process never went forward.

Finally, it is disconcerting that ICANN initially signaled that it will be publishing its own interim model merely two days following the comment period. ICANN now has announced that it will host a webinar in February after the close of comment period to allow more time for the community to provide feedback. Regardless, it seems that ICANN is operating on a fixed timeframe that does not allow sufficient time to review, analyze, synthesize, and harmonize the feedback and incorporate it into a solidly constructed model to recommend and implement.

**Conclusion**

According to Section 4.6(e)(i) of ICANN's Bylaws, ICANN is required to use "commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data." ICANN also has, as one of its stated remits, the duty to preserve the security and stability of the domain name system. Both obligations impose on ICANN a responsibility to guide the multi-stakeholder community in developing a WHOIS model that is GDPR compliant while preserving the current WHOIS data to the greatest extent possible.

Every day, Internet users, academics, consumers, registrars, registrants, governments, law enforcement officials, cybersecurity experts, and IP and brand enforcement companies all require access to WHOIS data in order to help ICANN preserve the security and stability of the DNS and ensure that the Internet ecosystem remains trusted and safe for Internet users around the world. Any interim model which fails to grant access to these groups for legitimate purposes not only violates ICANN's bylaws, the advice from the GAC stated in the Abu Dhabi Communique, but also the GDPR itself. MarkMonitor encourages ICANN to consider this feedback as well as comments from others before hastily publishing a deficient interim model which many may feel beholden to adopt.

Respectfully submitted,

A. Statton Hammock, Jr.
Vice-President, Global Policy & Industry Development
MarkMonitor, Inc.

January 29, 2018