DomainTools Comments on the 3 ICANN Compliance Models Published 1/12/18

On behalf of DomainTools, I appreciate the chance to comment on the ICANN Proposed Interim Models for Compliance With ICANN Agreements and Policies in Relations to the European Union's General Data Protection Regulation, published January 12, 2018.

DomainTools builds Enterprise-class threat intelligence solutions currently used by nearly 500 worldwide customers, including a third of the Fortune 100. Domain name Whois data is a key piece of the products our customers use every day to help defend their networks from ongoing cyberattacks. In business for nearly 20 years, DomainTools has developed an expertise in marshalling Whois data for effective use in the prediction, prevention, investigation and mitigation of network security threats.

DomainTools' feedback on these models is informed by these goals:

1. Retains Whois as close to its current form as possible, a goal ICANN Leadership has mentioned on multiple occasions.
2. Consistent with both the letter and the spirit of the GDPR regulation.
3. Has an implementation that is achievable by contracted parties.
4. Achieves all of the 5 Purposes outlined at the top of Page 6 of the ICANN memo.
5. Honors ICANN's important and enduring role in the stability and security of the DNS.

DomainTools makes these general observations and recommendations:
Because the RDS PDP will likely take some time to complete its journey, the "interim" period from May 25th 2018 onward may be lengthy. It is important therefore that ICANN and its Community are very thoughtful and thorough on the design of the interim Whois model.

It is imperative ICANN settle on one model as soon as possible. Registrars and Registries have been very public in stating that they have had to take matters into their own hands, and are already down the path of developing their own curated solutions for Whois compliance with GDPR. This is going to result in a fractured Whois system where each contracted party makes different data sets available in different ways and there is no clear expectation as to what if any data an Internet user will be able to see about who owns or controls a domain name. We need to avoid or minimize this type of outcome as much as possible. Consistency of data availability across registrars and registries is important to the efficacy of Whois data for the important use-cases it supports today. Indeed Page 6 of the recent ICANN memo on these models talks specifically about the importance of "uniform registration data".

We note that there is no mention of data validation or data accuracy enforcement in any of the models. A longtime criticism of Whois has centered on data quality, so any contemplated changes to Whois should address this shortcoming.

Of critical importance is the lack of any centralization of data and data access in any of the models. The legitimate interests of network and cybersecurity teams worldwide, teams specifically charged with protecting internet users and supporting trust in the DNS, are critically impaired without the ability to search across the aggregated Whois data set to make correlations that inform the prediction, prevention and remediation of cyberattacks. We strongly recommend that ICANN retain and enforce the requirement

for Port43 Whois service which has historically allowed bulk access to this critical data set.

DomainTools comments on the 3 Models published in the January 12 memo:
ICANN CEO Goran Marby commented during the January 24th IPC/BC Whois Discussion Event that the final model is likely to be a melding of aspects of the proposed models, including all of the original community-submitted models, and that ICANN is not specifically picking only from one of the three proposed models as is. Among the many thoughtful models submitted by the community, DomainTools most strongly supports the spirit and vision of the iThreat Model. However, because we are asked to comment specifically on the three resulting models proposed by ICANN, our position is that we would support ICANN's proposed Model 1 with the following comments or updates:

Natural Persons:
The GDPR makes it clear that there is an important delineation between Natural Persons and Legal Persons and Model 1 appropriately identifies Natural Persons as the only affected Registrant class.

For item "B" ("the registrar and/or registry are established outside the EEA and provide services involving the processing of personal data from registrants located in the EEA") we want to clarify that this language does NOT mean that if a non-EEA Registrar or Registry has SOME registrants in the EU that GDPR applies to ALL of that Registrar or Registry's domain registration data.

We note there is no mechanism in Model 1 to identify Natural Persons from Legal Persons or other. We propose an opt-in mechanism (simple check box) for domain registrants to self-identify as Natural Persons in the EU, as well as a follow-on validation process as suggested in the ICANN Redaction Proposal.

Minimum Public Data Set:
Email Address of the Domain Registrant should be included, as it is by far the most commonly used and lowest friction medium for communicating with the domain holder. We point out Purpose #1 which requires a "reliable mechanism for identifying and contacting the registrant". Email is clearly a more timely and reliable mechanism than mailing a letter to a physical address. Pursuant to the "identifying" requirement in the same Purpose #1, the Registry Registrant ID should also be included in the minimum public data set.

Data Retention:
Whois data remains relevant for legitimate use cases related to network and cybersecurity threat investigations, well beyond the two years proposed in Model 1. We suggest minimum five years here, and base that on actual Whois history usage data by security practitioners which we have proprietary access to.

Tiered Access:
Time-to-data is a critical element in network and cybersecurity work which are two important Purposes (#4 and #5) included on Page 6 of the ICANN memo. Any solution for tiered access must acknowledge the ability of certain parties to have near-real-time access to Whois data. The Model 1 solution that relies on the over 2,500 disparate Registrars and Registries to individually adjudicate certification and legitimacy of data requests will suffer from tremendous inconsistency of process, decisioning and

response. DomainTools supports self-certification by data requestors and suggests a centralized data access body with resources to scale and respond quickly, similar in spirit to what is proposed in the ICANN Redaction Proposal. We acknowledge that tiered access solutions are more involved and can be designed and implemented after the initial interim model is launched.

Concluding Comment:
Having worked hands-on with Whois data for nearly two decades, DomainTools has a unique orientation to this critical issue. In writing this comment, and in our increasing involvement in the community activities surrounding the future of Whois, we aim to represent the very legitimate and important interests of our worldwide security clientele who come to work every day trying to make their citizens, their employees, their customers, their users, and all internet constituents, including the very same people the GDPR aims to protect, safer from those that mean to do harm. On their behalf we appreciate this opportunity to submit these comments.

Respectfully,
Timothy Chen
CEO, DomainTools