USG Comments

ICANN's Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation

The United States Government (USG) appreciates this opportunity to comment on ICANN's Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's (EU's) General Data Protection Regulation (GDPR). At the outset, we want to confirm the USG's support for the comments submitted by the Governmental Advisory Committee (GAC). The following comments build off the GAC comments, providing emphasis and supplementary input to reflect the specific views of the USG.

Rather than select one of the proposed models or even build a model à la carte, the USG takes this opportunity to articulate its needs and expectations for a modified WHOIS that complies with GDPR. Specifically:

Model Applicability

- Regarding the models and the varied applicability in terms of who and where the model would need to apply (*i.e.*: European registrants versus all registrants; registrars/registries in Europe versus not in Europe; etc.), the USG expects a model that is global in nature.
    - For the sake of clarity and predictability for those implementing as well as the users of the information, a single model should be decided upon that does not make distinctions between registrants and jurisdictions.
    - A single, global model will also work to ensure the continued interoperability and authoritative nature of the WHOIS.
    - The USG cannot accept a situation whereby the WHOIS system is fractured, as it would undermine the public interest and ultimately the stability of the DNS.

Legitimate Purposes

- Any model should clearly recognize that all legitimate purposes for data processing should be permitted through the WHOIS service. This will provide clarity and predictability for WHOIS users as well as for those who are responsible for implementing the model.
- The USG would like to stress that legitimate purposes include those associated with law enforcement, IP rights protection, consumer protection, cybersecurity, anti-abuse/fraud, and other public safety purposes.

Information Collected

- The USG strongly supports a model that maintains the collection of thick WHOIS registration data for legitimate purposes.

Information Displayed

- The USG expects and supports a model that publically displays as much information as possible, recognizing that personal information (and only personal information) needs to be protected for purposes of complying with GDPR.
- That being said, it is critical that the Registrant's email also be publically displayed. This email enables a registrant to be quickly and effectively contacted. A physical address is not nearly as efficient. Further, having the additional information of an email address allows those involved in anti-abuse efforts to analyze for patterns among malicious registrations.
- In addition, the USG expects a model that makes a distinction between natural and legal persons. The GDPR does not require the protection of legal persons' information, and is therefore unnecessary. Not only does this preserve the public display of useful information for governments, IP rights holders, and cybersecurity firms, but this approach also makes more information available to consumers to verify the entities they are transacting with online.

Access to Non-Public Data

- Recognizing that to be GDPR compliant, some personal information will no longer be made public, access to that data should not be unduly restricted or overly burdensome for legitimate purposes. Moreover, a determination of what is not overly burdensome should have an empirical basis, taking into account actual experiences, and not be a conclusory assertion.
- The USG recognizes that a tiered access model would necessitate accreditation/certification, whether it is self-accreditation or through some other approach. It is the view of the USG that there needs to be enough flexibility to allow discrete categories of users to decide amongst themselves how best to achieve this, and not be dependent on judicial determinations or registrar decisions.

Data Retention

- Registries and registrars must be required to retain registration data for two years beyond the life of the domain name registration. This is the current standard in ICANN's contracts and there is no legal justification for why this needs to change.
- Historical WHOIS data is critical for an array of legitimate investigative purposes that serve the public interest. This is particularly the case for law enforcement and cybercrime investigations that are increasingly global in nature and involve a multitude of parties.
- Bulk access to third parties should continue to be required, as this is a critical tool for law enforcement and cybercrime investigators to determine patterns and conduct the appropriate analysis.

In closing, WHOIS can, and absolutely should, retain much of its current form while complying with national privacy laws, including the GDPR. It is in the interests of all Internet stakeholders that it does. The U.S. government expects this important information continue to be made quickly and easily available through the WHOIS service.