ICANN | ISPCP

Internet Service Providers & Connectivity Providers

The ISPCP thanks the GNSO Council leadership for their questions regarding whois information accuracy and offers the following elements for consideration on the “Threshold Questions for SG Exploration”:

- *What are concrete and articulable examples of what inaccurate data DOES prevent or inhibit, and how does it do so?*

  Inaccurate data may prevent:

  - “Delivery Status Notification (failed)” error messages received when emails are sent to whois Registrant Email, or calls not delivered to Registrant Phone or Fax. Accurate data only ensures that the message is delivered.
  - “connection failed” or “server not found” errors when registration server details are not accurate
  - When dealing with cybersecurity issues, ISPs need accurate information to trace malicious activities back to the responsible parties and anything that stands in the way of identifying the source is a problem, including inaccurate domain name whois data – requests for such identification may be internal to ISPs or may be requested to ISPs by law enforcement agencies
  - For example, ISPs may have to rely on accurate WHOIS data to identify and address abuse reports (e.g., spam, phishing). Inaccurate data can delay response times and hinder effective action against abusive users.
  - ISPs may struggle to assist customers with domain-related issues if contact information is incorrect. Ultimately this can result in poor customer service and dissatisfaction.

- *What are concrete and articulable examples of what inaccurate data does NOT prevent?*

  Inaccurate data does not prevent the following:

  - Individuals can register domains with false information, and the vast majority of what domain names are used for on the Internet is unaffected by inaccurate registration data information: use of a domain name for the web, email, search engine indexing, content creation, and the incentive for having accurate data other than compliance (contractual or regulatory) is very limited
  - accurate data does not prevent an email (eg regarding “DNS abuse”) from being dismissed or ignored.

- *Are there specific stakeholders, industries, or sectors particularly vulnerable to the effects of inaccurate registration data? If so, what are they and why?*

In the ISPCP's view, some stakeholders that may use registration data (among other sources) are more vulnerable to inaccurate data. : Financial Services, which are often targets for fraud and phishing attacks: law firms and compliance departments, which rely on accurate WHOIS data for legal actions and investigations; Government Agencies, which may need to track DNS abuse for cybersecurity purposes.Those may turn to ISPs for assistance as a result of not finding the information in whois

- *Given the examples provided in response to the three questions above (if any), please articulate a short problem statement for accuracy. The problem statement should consider:*
  - *What is the current problem or challenge?*
  - *What are the consequences of this problem or challenge?*
  - *What is the ultimate objective of working on this problem or challenge?*
  - *Considering the limitations of data processing, how do you propose to address this problem?*

Inaccurate whois data has existed since whois/DNS was created but having inaccurate and unusable data in a public database defeats the purpose of having a public database in the first place. We would suggest the actions to focus on incremental improvements and compliance/regulatory compliance. Processes may include:

- Enforce RAA provisions on accuracy (eg 3.7.7.2, 3.7.8 etc) and more generally the RDDS Accuracy Program Certification
- Validate data at registration, check accuracy at registration renewal, with a risk of administrative overhead
- Conduct technical checks and consider coercive measure such as suspension, if necessary
- Consider stronger registrar/registry coordinated effort?
- Promote 'KYC' (Know Your customer) on every renewal
- Automatic testing and regular audits to detect inaccuracy

Is now the appropriate time to address the problem? For example, some stakeholders have mentioned the implementation of NIS2 as an important precursor to understanding new accuracy requirements. Should this or other examples be considered prior to engaging in potential policy work?

We believe ICANN should continue addressing the problem, even with incremental changes which may not provide a solution to the complete problem space. Compliance to NIS2 and the experience of European ccTLD operators in particular, in that regard should be used in conjunction with other means to approach registration data accuracy but the timeline for the definition of measures to combat registration data inaccuracy should not be dependent on NIS2 implementation.

Are the ICANN org alternatives proposals worth exploring, such as:

- *Provision of historical audit data that measures registrars' compliance with accuracy-related provisions in the RAA.*
- *Engagement with contracted parties and ccTLD operators on developments in European policymaking regarding registration data accuracy.*

The ISPCP considers those proposals worth considering, especially the cooperation with ccTLD operators that may have already considered how NIS2 regulation should be complied with for what relates to data accuracy. Others such as the use of AI/ML tools may also be interesting.

What are the limitations of the ICANN proposals? Why should or should they not be pursued?

None of these would seem to offer avenues that could be considered in the short term.

What other possibilities can be explored to move our work on Accuracy forward?

Other avenues may be worthwhile considering such as improvement to standardized formats for WHOIS data to ensure consistency and ease of verification across registrars; partnerships between registrars and law enforcement to facilitate the reporting and resolution of abuse cases linked to inaccurate data; or feedback mechanisms to allow users to report inaccuracies in WHOIS data, with a process for timely resolution.