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

Registration data is a critical component in the domain name system, providing essential information about the registrant of a domain name. Accurate registration data is vital for various stakeholders, including law enforcement agencies, intellectual property owners, and cybersecurity professionals. Inaccurate registration data can significantly impact domain name enforcement in several ways:

Difficult in Identifying Registrants:

Accurate registration data allows for the identification of the individual or entity that registered a domain name. When this data is inaccurate, it becomes challenging to determine who is responsible for the domain. This can hinder efforts to enforce legal actions, such as serving cease-and-desist orders or pursuing litigation for trademark infringement.

Challenges in Cybersecurity Efforts:

Cybersecurity professionals rely on registration data to track down malicious actors who use domain names for phishing, malware distribution, or other abuses. Inaccurate registration data can obstruct these efforts, making it harder to mitigate threats and protect users from harm.

Obstacles in Intellectual Property Protection:

Intellectual property owners often use registration data to monitor and enforce their rights against domain names that infringe on their trademarks or copyrights. Inaccurate data can delay or complicate the process of taking down infringing websites, leading to prolonged unauthorized use of protected content or brands.

Compliance Issues:

Inaccurate data can result in non-compliance for registrars and registrants. ICANN requires that a registrant provide accurate registration data.

Impact on Trust and Credibility:

The integrity of the registration database is crucial for maintaining trust in the domain name system. Inaccurate data can undermine confidence in the system, affecting the credibility of domain name registrations and the entities that manage them.

Enforcement Delays and increased Costs:

Inaccurate registration data can lead to delays in enforcement actions as additional resources and time are required to verify the true identity of the domain registrant. This can increase the costs associated with enforcement efforts, making it more burdensome for affected parties, and essentially renders ICANN's commitment to access to meaningful registration data worthless. Anecdotally, IPC members have handled thousands of domain name disputes and estimate that in 90 to 95% of them the data leads to a fake name, fake address, fake phone number, and often an email address that is dubious as to its legitimacy. Statistically, an almost 15 year old report entitled, "*Study of the Accuracy of WHOIS Registrant Contact Information,*" developed for ICANN by NORC at the University of Chicago in 2010 found that "only 23% of

WHOIS records can be considered fully accurate." This is problem that has only gotten worse over the last decade and a half.

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

Learning that a domain name is registered, when it was registered, when it is set to expire or renew, and who the registrar is. This question is a bit of a red herring in that this data isn't helpful at identifying abusers as typically when inaccurate data is discovered after it is already known that a domain name is registered (why else would you learn of this)?

Are there specific stakeholders, industries, or sectors particularly

vulnerable to the effects of inaccurate registration data? If so, what are

they and why?

All Internet users are affected by inaccurate data. Those particularly affected include:

Cybersecurity Firms:

Threat Analysis and Mitigation - Cybersecurity firms rely heavily on accurate registration data to track down malicious actors, identify the origins of cyberattacks, and mitigate threats. Inaccurate data can hinder their ability to respond effectively.

Incident Response - During a cybersecurity incident, timely and accurate registration data is crucial for identifying compromised domains and taking appropriate action.

Law Enforcement Agencies:

Cybercrime Investigation - Law enforcement agencies use registration data to investigate cybercrimes, including fraud, identity theft, and other online criminal activities. Inaccurate data can impede investigations and delay justice.

Legal Proceedings - Accurate registration data is often required for legal processes, including serving legal notices and subpoenas.

Intellectual Property Holders:

Trademark and Copyright Protection - Companies and individuals protecting their intellectual property rely on registration data to identify and take action against infringing domains. Inaccurate data can make it difficult to enforce rights and protect brands.

Domain Disputes - Accurate registration data is essential for resolving domain name disputes through mechanisms like the Uniform Domain-Name Dispute-Resolution Policy (UDRP).

E-Commerce and Online Businesses:

Consumer Trust - E-commerce platforms and online businesses depend on accurate REGISTRATION data to build and maintain consumer trust. Inaccurate data can lead to fraudulent activities, damaging reputations and customer relationships.

Financial Institutions:

Fraud Prevention - Banks and financial institutions use registration data to detect and prevent fraudulent activities. Inaccurate data can lead to increased risks of fraud and financial losses.

Internet Service Providers (ISPs):

Network Security - ISPs use registration data to manage network security and address issues such as spam, phishing, and other malicious activities. Inaccurate data can compromise network integrity.

Domain Name Registrars and Registries:

Compliance and Accountability - Domain registrars and registries are responsible for maintaining accurate registration data. Inaccurate data can lead to compliance issues and affect their credibility.

Customer Verification - Accurate registration data is necessary for verifying the identity of domain registrants and preventing domain hijacking.

Inaccurate registration data can have far-reaching consequences across multiple stakeholders, industries, and sectors. Ensuring the accuracy of registration data is essential for maintaining cybersecurity, protecting intellectual property, fostering consumer trust, preventing fraud, and supporting compliance. Each of these stakeholders, industries, and sectors relies on accurate data to perform their functions effectively and safeguard their interests.

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:

o What is the current problem or challenge?

o What are the consequences of this problem or challenge?

o What is the ultimate objective of working on this problem or challenge?

The current problem is that most registrant data is inaccurate and despite having policies and contractual terms requiring accurate data, these provisions are not being enforced.

Inaccurate registration data can have far-reaching consequences. It allows criminals to use the Internet and DNS system to defraud the public, the rights of others to be infringed, and calls into question the work that the ICANN community has been engaged in for years on registrant data accuracy as access to inaccurate data doesn’t solve any of the underlying problems that the access debate has sought to address whether from access seekers or those seeking to shield the identity of registrants.

The ultimate objective is to have policies and contractual terms requiring registrant data that has been validated, i.e., syntactical, operational, and identify validation. See SAC058: SSAC Report on Domain Name Registration Data Validation.

Considering the limitations of data processing, how do you propose to address this problem?

Most of the problems around data processing are overstated and NIS2 is meant to address these overstatements with clear requirements. Upon completion of the implementation of NIS2, we need Contracted Parties to adopt voluntary commitments to comply with NIS2 and its accuracy and disclosure requirements. Should Contracted Parties not do so, we should begin an EPDP to develop new Consensus Policy that require validated registration data, access to that registration data, and a requirement for registrars to delete domain names from the DNS that have inaccurate data.