ICANN 72
Summary of WHOIS and Proxy Requests Under GDPR
DNS Abuse Framework Requests (YTD 2021)[1]

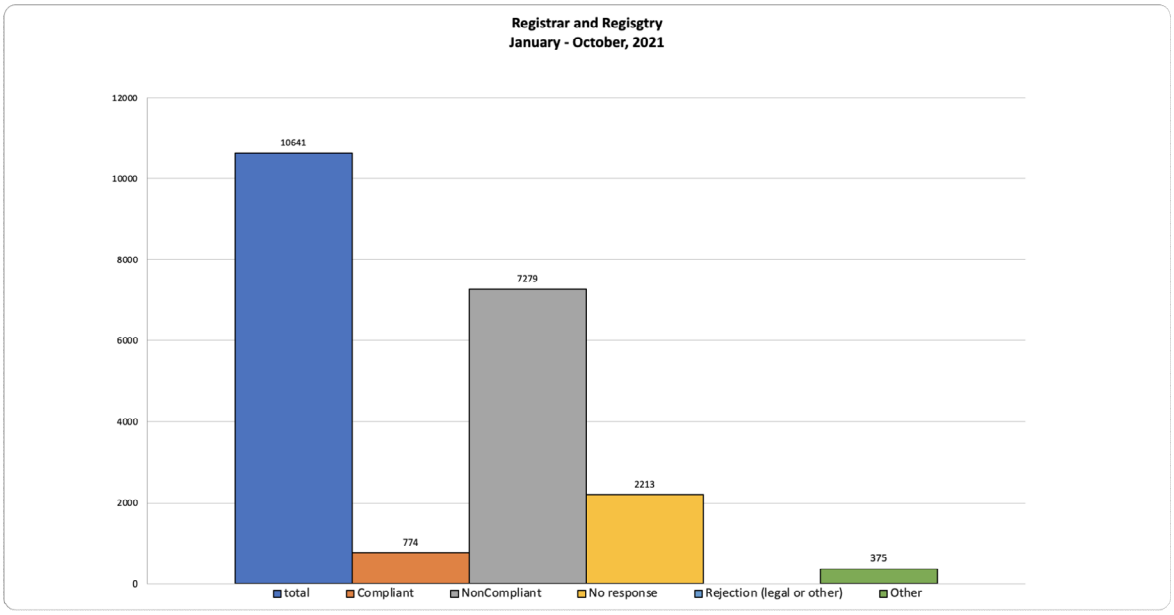
Summary

- The following overview summarizes response rates for WHOIS and Proxy data requests in 2021 from **two leading enforcement vendors and one law firm** on behalf of multiple clients and brands for well-documented and supported requests. Purposes cited in the requests included cybersecurity, DNS abuse, and IP infringement.
- **Total WHOIS requests: 10,641; Total Proxy requests: 4075**
- **93% of WHOIS requests to registrars and thick registries were not fulfilled - for an aggregate of 7% success rates**. This continues the downward trend seen over the last year- representing a significant decrease from the 20% success rate from ICANN 69.
- Notably, approximately 21% of all WHOIS requests result in no response at all.
- **93% of Proxy requests for the customer's contact data were unfulfilled**.
- Phishing-related requests or requests concerning obviously fraudulent domains are rarely fulfilled even for signatories of the Domain Abuse Framework**.**
- This is troubling in light of the 70% increase in phishing over the last year as reported by Interisle, which is concentrated among a small group of registrars.
- When phishers register domains, they tend to use them quickly – more than half within 48 hours. With compliant WHOIS reveal requests taking an average of 7 days, the data often comes too late to protect the public from fraud.
- **Initial 2021 year-to-date results for 257 requests to signatories of the DNS Abuse Framework: compliance rate of 85% among participating registrars, and 80% among participating registries.**
- Cybersecurity investigators are reporting struggles in identifying perpetrators and putting an end to criminal campaigns as a result of having little to no access to WHOIS data.
- The delays and roadblocks in WHOIS are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities.
- One major registrar has introduced significant fees for legitimate requests to redacted WHOIS, raising ICANN compliance concerns.

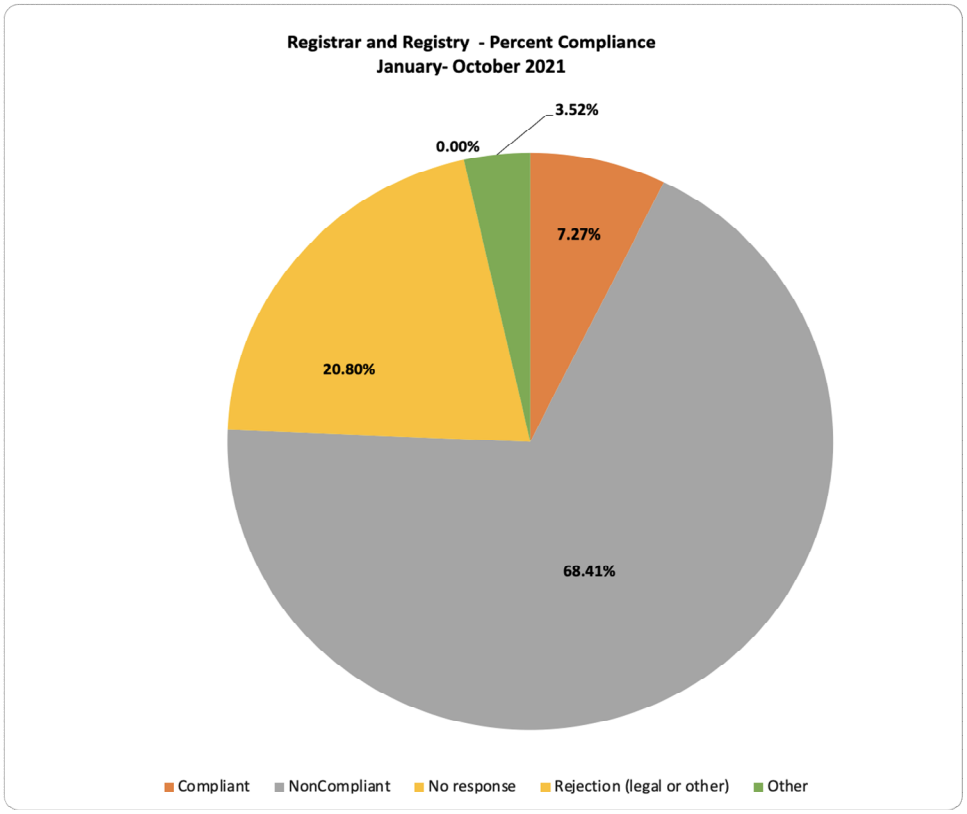
[1] Data through Sept 30, 2021

WHOIS Reveal Requests Results:

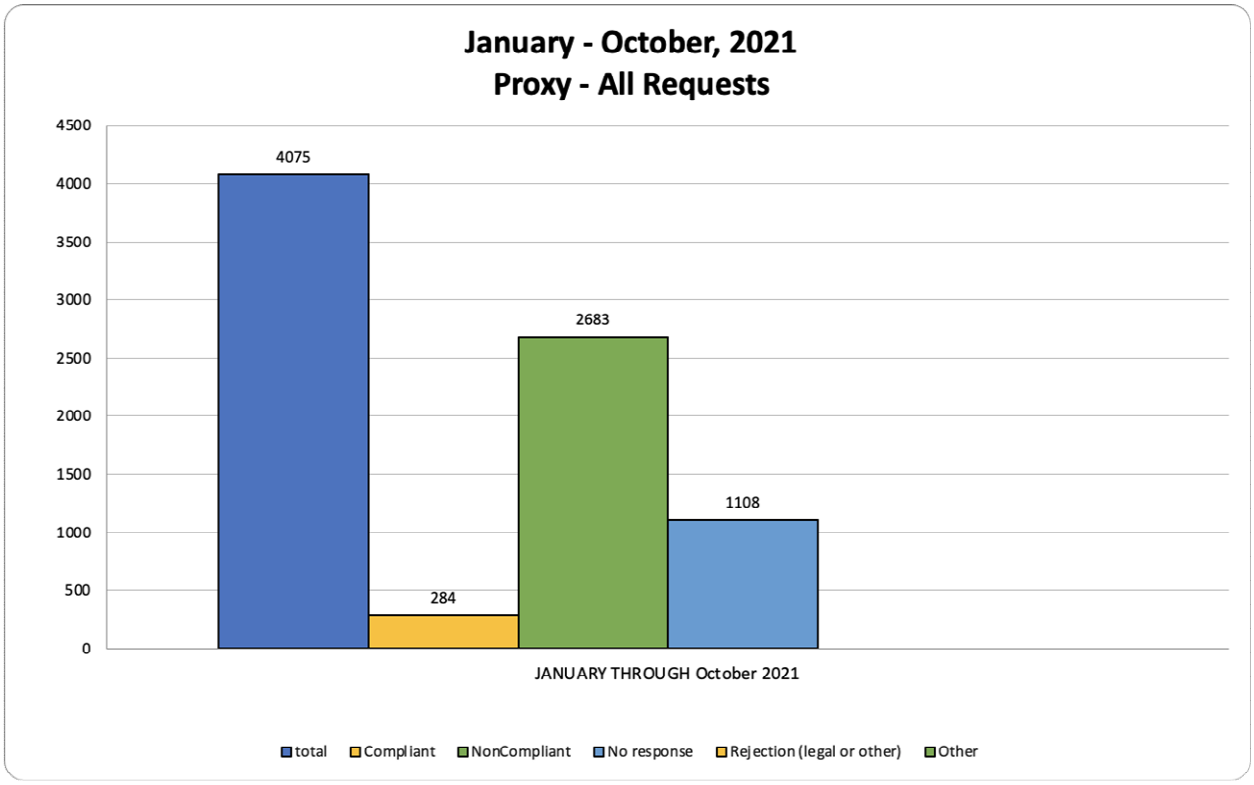
1. Registrar and Registry – All Results



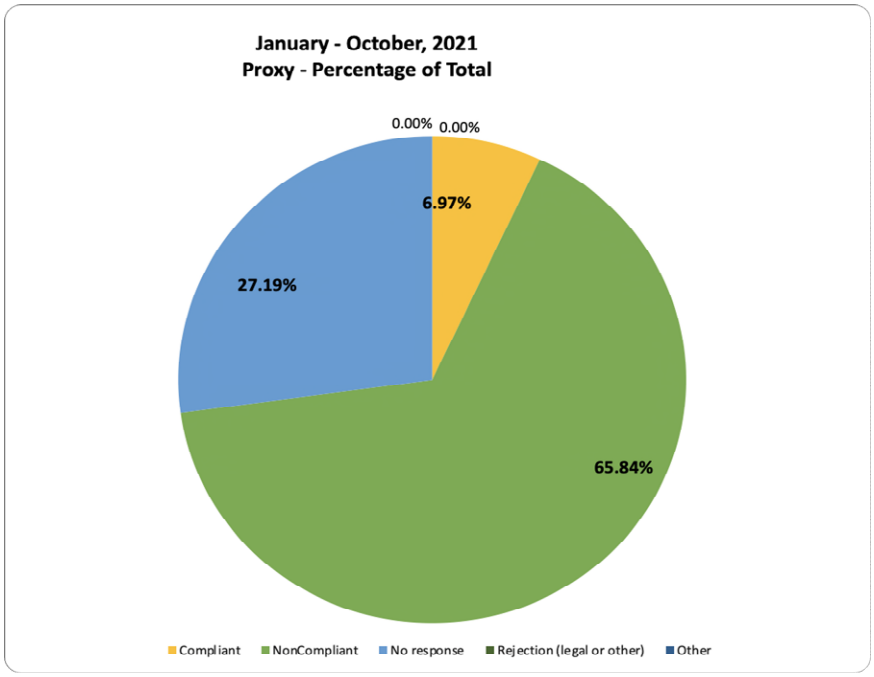
2. Registrar and Registry - Percent Compliance



3. Proxy - All Requests



4. Proxy - All Products - Percentage Compliance



Additional Information

- The Phishing Landscape Report, 2021 reports that most phishing is concentrated at small numbers of domain registrars and domain registries. 69% of the domains used for phishing were registered in 10 Top-level Domains and 69% were registered through just 10 registrars.
- Interisle reports that 57% of domains reported for phishing were used within 14 days following registration and more than half of those were used within 48 hours.
- The May 2021 Report "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later" by M3AAWG and The Anti-Phishing Working Group (APWG) reports:
    - Changes to WHOIS significantly impeded cyber applications and forensic investigations and caused harm or loss to victims of phishing, malware or other cyber attacks.
    - Response times are significantly longer, causing harm.
        - The need to request access to the non-public data elements introduces significant delays, usually days, in circumstances where mitigation prior to GDPR was accomplishable within a few hours.
        - These delays allow malicious activities to remain active and thus cause harm for longer periods of time.
    - Requests for non-public WHOIS by legitimate investigators for legitimate purposes remain ineffective. The disclosure of redacted WHOIS data is inconsistent; requests are often ignored or denied, and "revealed" data are often not actionable.
    - Dealing with ICANN compliance is a lengthy and inefficient process that too frequently results in no action.
        - 77% of responses - close to four out of five - express dissatisfaction with ICANN compliance.
        - Multiple respondents underline that they stopped submitting complaints to ICANN, as this constitutes a waste of their time.
    - There is no alternative to WHOIS - nearly 75% of respondents are unable to find alternative data sources to replace WHOIS.
- The "Interisle WHOIS Contact Availability and Registrant Classification Study" published in January, 2021 reports that application of the Temporary Specification has allowed the redaction of much more contact data than is required by GDPR - perhaps five times as much as is necessary.
- The voluntary DNS Abuse Framework by some registrars and registries is a welcome development, and is resulting in suspension of the domain name or removal of the nameservers.
- However, requests made in accordance with the DNS Abuse Framework were unnecessarily rejected where the malicious content was previously removed by the hosting company and no longer visible to the registrar. These requests should be fulfilled to prevent ISP hopping (where the website moves to another hosting provider).