BC INPUT TO THE EUROPEAN COMMISSION DG GROW

Response to Call for Evidence: EU Toolbox Against Counterfeiting

Our recommendations

The ICANN Business Constituency stands in strong support of the Commission's effort to step up the fight against counterfeiting and to clarify the roles and responsibilities of right holders, public authorities, and intermediaries, particularly domain name registries/registrars. There is currently a lack of accountability and clarity to incentivize these intermediaries to engage in the fight against counterfeiting beyond the fulfillment of minimum legal obligations when it comes to sharing with law enforcement authorities and rights holders the identifying information of *who is* behind a domain name or website implicated in the sale of counterfeit goods.

In the inputs to and the development of the Toolbox Against Counterfeiting the BC sees a number of opportunities for policymakers to (1) develop stronger accountability measures to mitigate Domain Name System (DNS) abuse and (2) provide legal clarity and new requirements for timely access to WHOIS data that is accurate and complete.

The BC supports recommendations from the Study on DNS Abuse that would

- require TLD registries, registrars, privacy or proxy providers and resellers to verify the accuracy of domain registration (WHOIS) data;
- encourage these same entities to develop and deploy new tools to identify domain names that could potentially infringe on their rights; and
- encourage these same entities to offer services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations.[1]

The BC also supports interlinked efforts to strengthen the Directive on measures for a high common level of cybersecurity across the Union (NIS2) in order to clarify and enforce a high standard for verification of accurate domain name registration data and require timely disclosure of WHOIS information, including in cases of online counterfeiting that exploit the DNS.

[1] "Study on Domain Name System (DNS) Abuse," p16.

Introduction and background

This response is provided on behalf of the Business Constituency (BC) of the Internet Corporation for Assigned Names and Numbers (ICANN), the not-for-profit public-benefit corporation dedicated to keeping the Internet secure, stable and interoperable. The BC is the voice of commercial Internet users within ICANN, representing the interests of small, medium, large and multinational enterprises as users of the Domain Name System (DNS).

The BC has played an active role in the multistakeholder community and other policy fora in attempting to address two critical and inter-linked issues that have plagued online safety for businesses and consumers:

I. the lack of accuracy of the WHOIS database and the lack of effective access to information in that database for law enforcement and other legitimate access seekers; and
II. the abuse of the DNS by a range of bad actors, including counterfeiters.

The Commission's Call for Evidence makes it clear that counterfeiting activities online are directly linked to both of these issues. When it comes to DNS Abuse, the Commission's recent Study on DNS Abuse puts some useful numbers to the problem, finding that over a two-year period, 25% of cases of abuse of the DNS involved websites selling counterfeit goods.[2] The study goes on to detail the links between counterfeiting and DNS abuse:

> "…voluntary initiatives taken by registries and registrars categorize domains used to host websites offering counterfeit goods, pirate content, or CSAM material as content-related abuse, thus, considering them falling outside of the DNS abuse. However, similarly to phishing or malware, the abusers may use DNS infrastructure, in particular, maliciously registered domain names to distribute such content in those abuse cases too."[3]

The Call for Evidence reiterates this link between counterfeiting and DNS abuse and spotlights the need for access to accurate and complete WHOIS data as part of guiding principle for facilitating effective and efficient information sharing (including personal data) in compliance with EU data protection and competition law, to prevent and detect counterfeiting activities:

> "…maintaining accurate and complete databases of domain name registration data (WHOIS data), and providing lawful access to such data for purposes related to the fight against domain name system (DNS) abuse, and ensuring that effective measures are taken to mitigate DNS abuse, including counterfeiting."

The BC wholeheartedly agrees with the Commission's assessment that accurate and accessible WHOIS data is necessary to help battle DNS abuse and counterfeiting. For years, we have

---

[2] European Commission, "Study on Domain Name System (DNS) Abuse," p55, January 2022: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1

[3] "Study on Domain Name System (DNS) Abuse," p52.

advocated alongside government and at-large stakeholders for reforms at ICANN that the institution has failed to act on. We have been engaged on – and remain wholly supportive of — potential regulatory and legislative remedies that are being developed in Europe, including the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2).

We would like to share some of our insights on the barriers to accurate and complete WHOIS data access, the issue of DNS abuse, and opportunities to positively impact both of these problems, and thus reduce counterfeiting online.

Our shared interest in curbing DNS abuse and ensuring access to accurate WHOIS data as a means to combat online counterfeiting

The Call for Evidence accurately details the ways in which counterfeiters and the organized crime networks that support them exploit weak systems and institutions, including:

> "…the lack of willingness of various intermediaries to engage beyond the fulfillment of minimum legal obligations, and of closer cooperation and information sharing between law enforcement authorities, right holders and other intermediaries."

The Call for Evidence goes on to rightfully include "domain name registrars and registries" in the scope of online and offline intermediaries. BC members have found precisely that these intermediaries lack engagement beyond the fulfillment of minimum legal obligations when it comes to sharing with law enforcement authorities and rights holders the identifying information of *who is* behind a domain name or website implicated in the sale of counterfeit goods.

The WHOIS database presents as an obvious system to solve this problem of access to accurate domain name registration information. However, for almost four years now, WHOIS accuracy and access has been debilitated by ICANN's reliance on domain name registrars and registries to interpret and apply the GDPR. The recent history of policy failure and its impact is clearly detailed in the Commission's recently published "Study on Domain Name System (DNS) Abuse":

> "On 17 May 2018, the ICANN Board adopted the Temporary Specification for generic top-level domain (gTLD) Registration Data (Temporary Specification) 228 intended to comply with EU's General Data Protection Regulation (GDPR), adopted in May 2018. The Temporary Specification provides modifications to existing requirements in the Registrar Accreditation (RRA) and Registry Agreements (RA) allowing registrars and gTLD registry operators to redact (withhold) personally identifiable data (and also those of legal persons) from publication in WHOIS. Further to the entry into force of the Temporary Specification, registries and registrars have consistently refused reasonable access to the redacted WHOIS data to third parties on request, such as law enforcement authorities or anti-counterfeiting organisations, and ICANN has stated that it is unwilling to enforce the Temporary Specification to require access in any case where a registry or registrar has refused it."[4]

[4] "Study on Domain Name System (DNS) Abuse," p102.

The BC and other stakeholders active in ICANN's multistakeholder community, including the Governmental Advisory Committee (GAC), where the EU is represented by the European Commission, have repeatedly warned, through public submissions, that the vital public interest and business needs of professionals engaged in cybersecurity, consumer protection, law enforcement, and intellectual property protection are consistently disrupted and sometimes simply unachievable because of inaccurate or inaccessible WHOIS information.

The Commission's Study on DNS Abuse highlights the impact in quantitative terms:

> "…the report on WHOIS Contact Data Availability and Registrant Classification Study 236, released on in January 2021, finds that ICANN's GDPR-driven policy has resulted in the redaction of contact data for 57% of all generic Top-level Domain (gTLD) names. ICANN's policy has allowed registrars and registry operators to hide much more contact data than is required by the GDPR-perhaps five times as much. Including 'proxy-protected' domains, for which the identity of the domain owner is deliberately concealed, 86.5% of registrants can no longer be identified via WHOIS-up from 24% before the ICANN policy went into effect."

The Commission's DNS Abuse study likewise comes to the grim conclusion that

> "The implications of this ICANN policy change are profound: consumers can no longer use WHOIS to confirm the identities of parties they may want to transact with on the Internet, it is harder for law enforcement personnel and security professionals to identify criminals and cybercrime victims, and brand owners face greater challenges defending misuse of their intellectual property."[5]

Strong privacy protections for personal data must be in place and adhered to, and the BC will stand behind policies and practices that strike a proper balance between the individual right to privacy and the safeguards necessary to ensure that legal obligations are met and that the public's safety is appropriately guarded.

But as it stands, the policies and practices that today determine access to WHOIS data simply "do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars, and those protecting the public from harms associated with bad actors seeking to exploit the domain name system." That was the conclusion of our colleagues on ICANN's Government Advisory Committee (GAC). We share this view and clearly see counterfeiting networks to be a major cohort of bad actors seeking to exploit the domain name system.

It's important to note that, repeatedly, we see other registries preserving privacy protections while facilitating sufficient public access to important data – for example, the EU trademark registry and countless business and property registries across Europe, all of which are compatible and consistent with GDPR. And some government-administered domain name registries in Europe have developed requirements, including through legislative means, to strike a balance that preserves privacy while also empowering law enforcement and other legitimate access seekers.

---

[5] "Study on Domain Name System (DNS) Abuse," p104.

The .eu registry is required to "organise, administer and manage the .eu TLD in the general public interest and ensure in all aspects of the administration and management of the .eu TLD", including for "high quality, transparency, security, stability, predictability, reliability, accessibility, efficiency, non-discrimination, fair conditions of competition and consumer protection."[6]

In Denmark, the Danish Domain Names Act requires that WHOIS data for ".dk" be made publicly available, even when the registrant is a natural person. The registry for .dk has publicly stated that the "purpose of this provision by the Danish legislators was to establish a high quality domain with as much transparency as possible."[7] And the experience of businesses, consumers, and other users of the .dk domain bears this out: according to Spamhaus statistics, .dk has a "badness" rate of .2% and a badness index score of .01 (compared to China's ".cn" that has a "badness" rate of 38.9% and a badness index score of 4.33).[8]

DK Hostmaster's success stands in stark contrast to the failures of accuracy and transparency that plague most registries operating outside of governmental requirements. For law enforcement and other users seeking legitimate access to WHOIS information, ICANN policy, or lack thereof, has instigated and is now sustaining a fragmented and unpredictable system, wherein each individual domain name registrar or registry conducts its own balancing test of issues that are clearly in the public interest, including counterfeiting.

A June 2021 survey of nearly 300 cybersecurity experts by the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG)[9] highlighted the ultimately futile reality that law enforcement and other legitimate access seekers face in requesting basic information on domain name registration:

> "94% of our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors."
>
> "Two-thirds of our respondents indicate that their ability to detect malicious domains has decreased."
>
> "The system to access redacted [WHOIS] data appears to fail regularly. Wait times are too long, while requests are being ignored, denied, or responded to with useless information."
>
> "Restricted access to Whois data by GDPR regulation under its initial interpretation hampers internet security; law enforcement activities; security research; anti-money laundering activities; and programmatic suppression of criminal infrastructure."

Our recommendations

The ICANN Business Constituency stands in strong support of the Commission's effort to step up the fight against counterfeiting and clarify the roles and responsibilities of right holders, public authorities, and intermediaries, particularly domain name registries/registrars.

---

[6] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58847

[7] https://www.icann.org/en/system/files/correspondence/vignal-schjoth-to-plexida-28may20-en.pdf

[8] See https://www.spamhaus.org/statistics/tlds/ last checked 28 February, 2022.

[9] Messaging Malware Mobile Anti-Abuse Working Group: "ICANN, GDPR, and the WHOIS: A Users Survey – Three Years Later," June 2021. https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

There is currently a lack of accountability and clarity to incentivize these intermediaries to engage in the fight against counterfeiting beyond the fulfillment of minimum legal obligations when it comes to sharing with law enforcement authorities and rights holders the identifying information of who is behind a domain name or website implicated in the sale of counterfeit goods.

From the NIS2 proposal and its ongoing negotiations, through the Toolbox Against Counterfeiting and the Study on DNS Abuse, the BC sees a number of opportunities for policymakers to (1) develop stronger accountability measures to mitigate DNS abuse and (2) provide legal clarity and new requirements for timely access to WHOIS data that is accurate and complete.

The BC supports the recommendation from the Study on DNS Abuse regarding **verification of accurate WHOIS Data**:

> TLD registries, registrars, privacy or proxy providers and resellers should verify the accuracy of the domain registration (WHOIS) data.

The BC also supports the study's recommendations on **new tools to assist legitimate access seekers:**

> TLD registries are encouraged to develop or improve existing similarity search tools or surveillance services to enable third parties to identify names that could potentially infringe their rights
>
> TLD registries are encouraged to offer, directly or through the registrars or resellers, services allowing intellectual property rights (IPR) holders to preventively block infringing domain name registrations.[10]

The BC supports the **recognition of legitimate access seekers** on the basis of rights holders, who seek disclosure of WHOIS data for the purposes of intellectual property investigations, enforcements, and legal actions, including fighting piracy and counterfeits to protect the public from harm. **Timely disclosure of WHOIS information** to legitimate access seekers is essential to facilitate law enforcement and investigations of online counterfeiting that exploits the DNS.

The BC supports **provisions in NIS2 that will restore the value of the WHOIS database for the Internet community.** To achieve this goal, the final Directive should include three critical requirements of Top-Level Domain registries and entities providing domain name registration services:

1. that they collect and maintain accurate, verified and complete domain name registration data;
2. that they make non-personal WHOIS data publicly available without undue delay; and

[10] "Study on Domain Name System (DNS) Abuse," p16.

3. that they provide access to specific domain name registration data, including personal data, upon duly justified requests of legitimate access seekers.

The NIS2 Directive can clarify a high standard for verification of accurate domain name registration data and ensure that the rights of legitimate access seekers extend to stakeholder groups involved in the prevention and detection of crime and fraud, including counterfeiting and other DNS abuse.