In re: Impersonation NPRM, R207000 **December 16, 2022**	)))))))	**Comments of The Coalition for Online Accountability ("COA")**

J. Matthew Williams
Mitchell Silberberg & Knupp LLP
1818 N St. NW, 7th Floor
Washington, DC 20036
mxw@msk.com
202-355-7900
Executive Director and Legal Counsel to COA

The Coalition for Online Accountability[1] ("COA") is pleased to submit these comments to The Federal Trade Commission ("FTC"). COA is a longstanding group of companies, trade associations, and copyright member organizations dedicated to enhancing and strengthening online transparency and accountability by working to ensure that domain name and IP address WHOIS databases remain publicly accessible, accurate, and reliable, as key tools against online infringement of copyrights, as well as to combat trademark infringement, cybersquatting, phishing, and other illegal acts. There is no doubt that the motion picture, music and videogame industries have long suffered from widespread online piracy and other abuses. COA members are seeing deceitful use of their company logos, brands, and copyrighted works, such as: in bogus job postings used for phishing schemes; to sell pirated content, NFTs, or cryptocurrency; or to push vaping products (which could target underage users). Increasing the regulatory tools that should help to thwart such conduct and impersonations of governments and agencies is of great importance to COA's members. In these brief comments, we focus on the issues of most relevance and significance to our coalition and industries, and do not respond to every question in the NPRM. We thank the FTC for considering our input.

Upon the effective date of the European Union's General Data Protection Regulation ("GDPR") and the Internet Corporation for Assigned Names and Numbers' ("ICANN") unilateral imposition of the Temporary Specification for gTLD Registration Data (the "Temp Spec")[2] in 2018, ICANN expressed a commitment to "comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible." However, the WHOIS system has not been preserved to the greatest extent possible

[1] COA comprises Broadcast Music, Inc. ("BMI"), Entertainment Software Association ("ESA"), Motion Picture Association, Inc. ("MPA), NBCUniversal, Recording Industry Association of America, Inc. ("RIAA"), The Walt Disney Co., and Warner Bros. Discovery.

[2] https://www.icann.org/resources/pages/gtld-registration-data-specs-en/

while still complying with the GDPR. On the contrary, there now exists a significant gap between the level of data access permitted under the GDPR and the real-world availability of WHOIS.

This situation with respect to lack of access to WHOIS data is due to registration data availability being severely limited by registrars and registries ("contracted parties"). Contracted parties are ignoring or not fulfilling legitimate data requests or are imposing procedural or legal hurdles that make securing access impracticable. This is consistent neither with the commitment to preserve the pre-GDPR WHOIS system to the greatest extent possible nor with the current contractual specification for contracted parties to provide "reasonable" access to legitimate data seekers. There is no justification for the redaction of data of legal person registrants or the overwhelming denial of reasonable access to personal WHOIS data for legitimate third-party interests as permitted under the GDPR and as set forth in ICANN's own Temp Spec. Artificial restriction of WHOIS data availability has had a profoundly negative impact on the health of the domain name system ("DNS"). International law enforcement authorities, cybersecurity investigators, intellectual property rights holders and others are unnecessarily hindered in their ability to investigate and ultimately mitigate behavior that is damaging to the DNS ecosystem and Internet users broadly (and at a time of rapidly rising rates of DNS abuse in many key categories, such as phishing).

This all aids and abets bad actors seeking to use the DNS to impersonate governments, businesses and other persons. In truth, there is very little disclosure occurring at all, even when disclosure requests are reasonable, legitimate, timely, well-founded, supported by evidence, and the interests of the access seeker clearly outweigh privacy concerns of the data subject.

In fact, it is extremely difficult to retrieve non-public WHOIS data for any reason. We refer you to ICANN's letter[3] to US Food and Drug Administration ("FDA") Commissioner Robert Califf, which stated, in part:

> *It is not necessary to obtain a subpoena to gain access to non-public domain name registration data. Law enforcement and consumer protection agencies around the globe have relied on existing ICANN WHOIS policies to gain access to this data.*

The FDA's explanatory reply[4] was direct in stating that -- in its experience -- this is not factual. According to the FDA's letter:

> *Unfortunately…this is not the actual experience of FDA-OCI special agents who, when requesting non-public domain name registration data from any one of the over 2,400 ICANN-accredited registrars operating globally, are often asked to submit a subpoena, court order (sometimes within the jurisdiction of the registrar), or Mutual Legal Assistance Treaty (MLAT) to obtain such information.*

The FDA's experience comports with that of COA's members and other similarly situated parties. Indeed, despite statements by ICANN to the contrary, nearly every legitimate disclosure request submitted by or on behalf of COA's members has similarly and unnecessarily been met with demands for subpoenas or court orders or, worse, ignored outright.

---

[3] https://www.icann.org/en/system/files/correspondence/marby-to-califf-14jun22-en.pdf
[4] https://www.icann.org/en/system/files/correspondence/hermsen-to-marby-15jul22-en.pdf

Due to this unfortunate state-of-affairs, COA believes that the FTC's regulations should be expanded to specifically address unauthorized creation/use of Internet identifiers, such as gTLD and ccTLD (e.g., .US) domain names, apps, and blockchain-based identifiers to impersonate businesses and governments. They should also include mitigation of "DNS Abuse",[5] the intentional registration and use of domain names for the purpose of impersonating, misleading or defrauding. Registrars and registries should be required to be responsive to abuse-related takedown requests that include credible evidence of abuse. The Rule should explicitly recognize as a "means and instrumentality" the failure to disclose non-public domain name registration data by a domain name registrar, registry operator, or privacy/proxy service provider upon receiving a credible request for such data in relation to impersonation being perpetrated through the relevant domain.

We again thank the FTC for considering our comments.

[5] COA supports the approach to defining DNS Abuse taken in the EU's January 2022 *Study on Domain Name System (DNS) abuse*: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.