

Congress of the United States
Washington, DC 20515

December 14, 2022

The Honorable Alan Davidson
Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave N.W.
Washington, D.C. 20230

Administrator Davidson,

We are writing to express our concerns with ongoing efforts to modify the contractual obligations for WHOIS between the United States government and GoDaddy for the management of the United States' country code top-level domain (ccTLD), .US WHOIS. Currently, GoDaddy is required to ensure that the .US WHOIS domain name registrant information is accurate and accessible in the interest of public safety and consumer protection.¹ For more than a decade, Congress has been hard at work on issues of data privacy and online consumer safety. Until Congress passes a privacy bill that addresses these issues, it is not appropriate for the NTIA to pursue the European Union's General Data Protection Regulation (GDPR) position over the United States' existing position.

Domain registration information, also known as "WHOIS," is critically important to protecting consumers online, ensuring our nation's cyber and national security, as well as combatting online criminal activity, including human trafficking and illegal online pharmaceuticals. WHOIS information informs consumers *who is* behind a domain name or website – similar to a land / title record. Prior to 2018, this information for .com and .net domain names were publicly and readily available to anyone who sought to verify *who is* on the other side of the computer screen. Unfortunately, as a result of an overly broad interpretation of the GDPR, this information is no longer easily accessible on domains outside of certain ccTLDs.

Countries are permitted to establish whatever rules they choose for managing their own ccTLDs. It has long been the policy of the United States to require verification and the publication of WHOIS information when registering domains on .US. Removing these requirements in the .US space would further invite bad actors to this platform due to the resulting lack of transparency. This ultimately would harm consumers as scams using the .US domain proliferate. These actors also would be emboldened by having a domain ending in .US, which many consumers view as an official United States government domain, like .GOV.

It has long been the position of the United States government to support accurate, accessible WHOIS information, not only for its own .US ccTLD but also for generic Top-Level

¹ https://www.ntia.doc.gov/files/ntia/publications/us_contract_june_28_2019.pdf

Domains, such as .com and .net. As such, efforts to remove WHOIS requirements from the .US country code would incorporate policies previously *rejected* by the United States government for the broader Internet, and run contrary to the goals of increasing consumer protection and protecting the public from harms.

Numerous cybersecurity studies and surveys have been performed in the wake of restricted access to WHOIS information since 2018 in the generic Top-Level Domains. In 2021, the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) conducted a users' survey targeting cyber investigators and anti-abuse service providers to, "determine the impact of ICANN's implementation of the EU GDPR." The survey found:

"From our analysis of 277 survey responses, we find that respondents report that changes to WHOIS access continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks."

In addition, the survey found that 94% of our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors. Finally, two-thirds of respondents indicated that their ability to detect malicious domains has decreased.²

Several federal agencies also responded to a congressional inquiry in 2020 on the impact that the loss of WHOIS information had on their investigative and enforcement capabilities. Highlights from those responses include the following:

- The **United States Food & Drug Administration** stated, "Access to WHOIS information has been a critical aspect of FDA's mission to protect public health. Implementation of the E.U. General Data Protection Regulation has had a detrimental impact of FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients."³
- The **Federal Trade Commission** indicated, "Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud."⁴
- The **U.S. immigration and Customs Enforcement Homeland Security Investigations (HSI)** and the **National Intellectual Property Rights Coordination Center (IPR Center)** said, "HSI uses domain registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII])

² https://apwg.org/m3aawg_apwg_whois_user_survey_report_2021/

³ [fda_whois_response.pdf \(house.gov\)](#)

⁴ [ftc_to_rep._latta_-_whois.pdf \(house.gov\)](#)

and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.”⁵

Congress, too, is on record supporting accessible WHOIS information. in the *Consolidated Appropriations Act for 2021* (P.L. 116-260), Congress included the following provision:

“NTIA is directed, through its position within the Governmental Advisory Committee, to work with ICANN to expedite the establishment of a global access model that provides law enforcement, intellectual property rights holders, and third parties with timely access to accurate domain name registration information for legitimate purposes. NTIA is encouraged, as appropriate, to require registrars and registries based in the United State to collect and make public accurate domain name registration information.”⁶

Thus, any attempt at this time to remove WHOIS information requirements from the contractual obligations around .US would be contrary to this direction, would take sides in a larger ongoing Congressional policy debate, and would be *harmful* to consumer privacy by exposing more consumers to phishing schemes, malware, and other cyber-attacks.

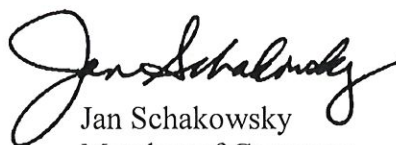
Additionally, we write to request copies of the annual WHOIS Accuracy and the Security Audit Data annual reports conducted by the .US Contracted Parties (Neustar and GoDaddy), as required under the same .US contract. We also request that the National Telecommunications and Information Administration provide us with any documents created by, and details of, its internal processes of its .US oversight obligations, including domain name abuse associated with the .US ccTLD. Requirements to provide accurate, accessible WHOIS information are currently included in the contract to manage the .US domain⁷. Also included are requirements to conduct and file a series of annual reports, including a WHOIS Accuracy Report. Please provide all such reports and documents dating from 2015 onwards to the signatories no later than January 13, 2023.

Thank you for your attention to this issue.

Sincerely,



Robert E. Latta
Member of Congress



Jan Schakowsky
Member of Congress

⁵ https://latta.house.gov/uploadedfiles/ices_signed_response_to_representative_latta.pdf

⁶ <https://www.govinfo.gov/content/pkg/CREC-2020-12-21/pdf/CREC-2020-12-21-house-bk3.pdf>

⁷ <https://www.ntia.doc.gov/page/2011/us-domain-space>