

March 25, 2021

The Honorable Michael Doyle, Chairman
House Energy & Commerce Committee
Subcommittee on Communications & Technology
Washington, D.C. 20515

The Honorable Robert Latta, Ranking Member
House Energy & Commerce Committee
Subcommittee on Communications & Technology
Washington, D.C. 20515

The Honorable Janice Schakowsky, Chairman
House Energy & Commerce Committee
Subcommittee on Consumer Protection & Commerce
Washington, D.C. 20515

The Honorable Gus Bilirakis, Ranking Member
House Energy & Commerce Committee
Subcommittee on Consumer Protection & Commerce
Washington, D.C. 20515

Chairs Doyle and Schakowsky and Ranking Members Latta and Bilirakis:

On behalf of the Coalition for a Secure & Transparent Internet (CSTI) we write in support of the Committee's ongoing efforts to address disinformation campaigns, both on social media platforms and across the Internet.

CSTI was founded in 2018 by a diverse set of stakeholders who shared similar concerns over the potential impact the implementation of the European Union's General Data Protection Regulation (GDPR) would have on the ability to ensure timely access to WHOIS information.

WHOIS information has historically been used by law enforcement, consumer advocacy groups, third-party investigators, intellectual property holders and others to identify *who is* behind a domain name or website. If the registrant of a website or domain is conducting illegal or otherwise malicious activity, investigators can access information about the registrant to pursue legal avenues as well as identify other, potentially dangerous domains that are also attributed to that registrant. In this way, WHOIS is critical to our ability to identify, end as well as proactively prevent cybercrimes, exploitation, fraud (including disinformation), intellectual property theft and other harmful activity.

As the Committee continues to examine these issues, CSTI encourages it to consider how WHOIS can help *identify* bad actors involved in these disinformation campaigns; the need for WHOIS information to *connect* participants engaged in these campaigns; and the role WHOIS plays in *shutting down* such campaigns.

Several Executive branch agencies shared their views on this subject in response to Congressman Latta's inquiries last year and their comments are worth noting. In its July 2020 response to Congressman Latta, the U.S. Federal Trade Commission said:

"Before the GDPR took effect in May of 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."



In its response to Congressman Latta (also in July of 2020), the U.S. Immigration & Customs Enforcement Homeland Security Investigations and the National Intellectual Property Rights Coordination Center said this regarding WHOIS:

“HSI uses domain name 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 the theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.”

Copies of these letters are enclosed.

Facebook, which is not a member of CSTI but is testifying today, has also expressed its concerns over the loss of WHOIS and the impact it has on protecting its own users. In a September 2020 letter to the National Telecommunications & Information Administration the company noted:

“WHOIS information and access is critical to protect the Facebook family of products from cybersecurity threats and fraud. Ensuring that WHOIS data is accurate, uniform, and easily accessible is key to our efforts to identify bad actors that target our platform and users with things like fake news, phishing attacks, brand infringement, and other malicious activity.”

A copy of the letter is enclosed.

The restoration of open, accessible WHOIS information will greatly enhance the ability of law enforcement, consumer advocates and others to identify and put an end to disinformation campaigns on social media platforms and across the Internet.

We thank you for your consideration of this important issue and stand ready to work with you and your staff moving forward.

Sincerely,

The Coalition for a Secure & Transparent Internet

Enclosures