

April 5, 2021

Dear US Stakeholders Council,

On behalf of the Coalition for a Secure & Transparent Internet (CSTI) we write in response to the open public comment period for the [usTLD Recommendation for Privacy Plan](#). CSTI opposes the underlying recommendation to allow privacy proxy services on the .US TLD and believes that doing so will leave Internet users *more* vulnerable to criminal activity.

CSTI was founded in 2018 by a diverse set of stakeholders who support open access to WHOIS information. Our members include organizations who come to this conclusion from a variety of issues areas – illegal online pharmaceutical sales, cybersecurity, human trafficking and sexual exploitation, consumer protection and intellectual property theft. The coalition was formed over the impact the implementation of the European Union’s General Data Protection Regulation (GDPR) would have on the safety of our Internet, and these underlying issues. Over the last few years, our concerns have been realized as the loss of this information has led to a more dangerous Internet for individuals.

As you know, 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. The loss of access to this data has significantly slowed the ability of law enforcement to respond to criminal activity, link criminal actors and their websites together and proactively block harmful websites before they can prey on Internet users. These conclusions are not only those of CSTI and its members but come from a variety of law enforcement agencies who responded to Congressional inquiries in 2020 about the importance of WHOIS, the role it plays in their investigations and prosecutions and the loss of timely access to this information.

In its response to Congressman Latta’s inquiry, the U.S. FDA commented that, *“Access to WHOIS information has been a critical aspect of FDA’s mission to protect public health.”* The agency added, *“WHOIS data has also been widely used in FDA’s criminal investigations to identify individuals and organizations selling online a variety of unapproved / uncleared / unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients.”*

The U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (HSI) also spoke to the importance of WHOIS saying, *“HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud.”* HSI noted that they, *“[use] 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.*” HSI’s focus on cyber crimes and the vulnerabilities that a lack of WHOIS information creates for individuals’ PII is especially noteworthy.

The U.S. Federal Trade Commission also responded to the inquiry on the role of WHOIS information by saying, *“The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims.”*

The loss of broad access to WHOIS information has made the Internet less safe. Enabling privacy proxy services to be used on the .US TLD would further exacerbate this problem and is the wrong policy for protecting Internet users. Again, CSTI would point to the various agencies who have historically utilized this information to carry out their respective functions. In the Congressional inquiry, the agencies were asked if they would support *greater* access to WHOIS information.

- The FTC indicated it would, *“benefit from greater and swifter access to domain registration data.”*
- HSI said that, *“If [it] had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminal move their activity to a different domain.”*
- FDA indicated its Health Fraud Branch would, *“be able to more quickly and efficiently identify and respond to the unlawful sales of FDA-regulated products if complete and accurate WHOIS data were available.”*

The functions these important agencies carry out are replicated and complemented by state and local law enforcement, cyber security professional and consumer protection advocates across a wide variety of issues.

CSTI appreciates the opportunity to respond during this comment period and has attached the above-referenced letters for your review and consideration.

Sincerely,

The Coalition for a Secure & Transparent Internet

Enclosures