July 16, 2018

Attn: Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, District of Columbia 20230

RE: *International Internet Policy Priorities* [Docket No. 180124068-8068-01]

Ms. Alexander:

On behalf of the Coalition for a Secure and Transparent Internet (CSTI), we are pleased to submit the following comments in response to the National Telecommunications and Information Administration's (NTIA) Notice of Inquiry on International Internet Policy Priorities.

CSTI was founded in April 2018 by leaders of DomainTools, LegitScript, and Spamhaus in response to concerns surrounding the impeding implementation of the European Union's General Data Protection Regulation (GDPR) and its potential impact on the WHOIS database remaining open and accessible moving forward. CSTI has grown to involve additional companies, nonprofits, trade associations, academics and others who are aligned in support of open access to WHOIS data. All CSTI members agree on the following general principles:

1. Open access to WHOIS is a critical tool in network and cyber security, consumer protection, brand protection, IP enforcement, and anti-abuse on the internet. Losing open access to WHOIS will curtail the success of these legitimate security, policy and social objectives.
2. Governments and law enforcement are just a few of the stakeholders that rely on the ability to access and maintain WHOIS data. Corporations, consumers, security researchers, reporters, brand owners, anti-abuse / compliance firms, and their partners also have legitimate interests in this data.

Our goal, as a coalition, is to ensure the WHOIS database remains open and accessible and we believe this should likewise be a priority for NTIA moving forward.

The Importance of WHOIS database and the Threat of GDPR

The WHOIS database is crucial for preserving transparency and understanding domain name ownership. Law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigations, copyright and trademark holders, journalists, academics, and others rely on WHOIS to help determine who is operating a criminal website, sending malicious (SPAM, phishing) emails, or initiating cyber security attacks. Companies and consumers also

rely on accessible WHOIS data, directly and derivatively, to determine who they are buying goods or services from.

In response to the EU GDPR, ICANN issued interim interpretation guidance that has attempted to provide a pathway for compliance. Unfortunately, this guidance threatens the integrity and transparency of the Internet and the way WHOIS data can be accessed and used. ICANN has stated it wants to modify the WHOIS system to ensure compliance with the GDPR while maintaining access to WHOIS data to the greatest extent possible. However, ICANN's own interim proposal undermines this goal.

As you know, the GDPR is intended to offer privacy protections only to "natural persons" of EU countries. The European Commission has made clear that "the GDPR only applies to personal data of natural persons and therefore does not regulate the processing of the data of legal persons (unless such data also relates to an identified or identifiable natural person)." In fact, the Commission explicitly stated that it "welcomes the distinction between personal data and other data (about legal persons)."[1] As such, ICANN need not allow registries and registrars to summarily restrict or throttle WHOIS data access in all cases.

Domain name registrars and registries worldwide, who initially collect and therefore control the WHOIS data, are on a course to restrict access to major elements of the WHOIS record, including name, email address, and telephone number of the domain name registrant. Although ICANN has proposed retaining access to a few data points, such as the registrant's organization (if any), state or province, and country, there remains a risk that even these will become mostly unavailable as registrars and registries are left to make their own decisions as to what is or is not compliant.

The Internet has thrived on the notion that distant commercial entities can be identified and therefore trusted, even as data flows over different networks and geographic boundaries. Creating different tiers of WHOIS access would splinter the Internet into "gated" communities, private enclaves, and proverbial back alleys. This would undermine the transparency of the Internet, stunt e-commerce, and create criminal safe-havens online.

As such, CSTI believes that registries and registrars ought to be required to treat the WHOIS data of legal persons and registrants using websites and emails to sell goods and services (collectively "commercial use registrants") differently than they do for the WHOIS data of EU natural persons who are afforded privacy rights under the GDPR.

The Need for a Solution

The GDPR includes an enforcement mechanism that threatens registrars and registries in non-compliance with very strict monetary penalties. This threat, and the lack of any countervailing law, puts registrars with access to this information in a difficult position, particularly with an evolving landscape and the questions raised by ICANN's interim guidance and the position of the European Data Protection Board. Simply put, registrars and registries are faced with the choice of restricting access to WHOIS information with no penalty ***or*** attempting to navigate an uncertain and evolving environment

[1] See https://www.icann.org/en/system/files/files/gdpr-comments-european-commission-union-icann-proposed-compliance-models-07feb18-en.pdf, page 3.

with the potential of catastrophic EU fines if they are not successful. **CSTI believes that the United States should enact legislation preserving open access to WHOIS data of commercial actors that intersect the U.S. public and consumers, and provide registrars and registries greater protections and motivations to continue to publish this critical information on as many domains as legally permissible.**

CSTI urges US policymakers to focus attention on domain name registries and registrars that impact Americans' online security, safety, and commercial interests. Specifically, U.S. policy should address domain name registration services (or that sells or resells domain names) *and* involves commerce among States, *or* registers domain names for any natural person of the U.S., *or* registers domain names to market or sell goods into the U.S. and any legal person. These registries and registrars should be required to publish in a publicly accessible WHOIS registration directory the same registrant data they made available prior to the GDPR-inspired cutbacks in public access for each domain name that it administers. Such WHOIS data should be required to be accurate, transparent, available at no charge, and not anonymous or masked unless the registrant is not using the domain name for commercial purposes and chooses to use an eligible privacy/proxy service[2].

How NTIA Can Help

We greatly appreciate the actions and comments of NTIA on this issue to date. Your efforts are so important and valuable.

NTIA can further assist by helping to educate lawmakers and key decision-makers on the importance of the WHOIS database and the need for action. NTIA can also assist this effort in providing feedback to legislative solutions as they materialize to ensure that the solution is practical, effective and enforceable. NTIA has a clear understanding of the importance of this tool and the potential dangers of it going away or being minimized in any way and lawmakers respond to the agency's expertise.

Thank you for your attention and efforts to help ensure the WHOIS database remains open and accessible in order to help protect Internet users from online criminal activity and to enable action against network and cyber security risks, intellectual property violations, and consumer fraud and abuse online.

Please contact CSTI anytime directly via Libby Baney (libby.baney@faegrebd.com) and Josh Andrews (Joshua.Andrews@faegrebd.com). We look forward to working with you on this important issue.

[2] CSTI recommends the definition of "eligible P/PSPs" be drawn from the standards for the Internet Corporation for Assigned Names and Numbers (ICANN) Privacy/Proxy Services Accreditation Recommendations dated December 7, 2015.