National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230

November 9, 2018

Re: Docket No. 180821780–8780–01

To Whom It May Concern:

The Coalition for a Secure and Transparent Internet (CSTI) is pleased to provide comment on the National Telecommunications and Information Administration's approach to consumer privacy. Consumer privacy is an increasing concern, particularly over the Internet, given the interconnected nature of our society across products and platforms where data is being collected and utilized for various purposes. As a coalition, we believe that the ongoing existence of an open, accessible WHOIS database is vital to creating a safer, more transparent internet environment that ultimately protects consumer privacy by helping in the detection, prevention and investigation of cybercrime which often results in unlawful access and monetization of personal data of US citizens. WHOIS data is a critical component of enterprise security, and core to anti- malware, spam, and phishing services which prevent internet users' online activity and information from being tracked, stolen, or abused. For these reasons, CSTI recommends that NTIA's efforts on online privacy include a recommendation to require WHOIS data transparency.

Led by DomainTools, LegitScript, SpamHaus, and the Motion Picture Association of America, CSTI is comprised of companies, nonprofits, trade associations, academics and others who support open access to WHOIS data. CSTI is concerned because, due to an overly broad interpretation of the European Union General Data Protection Regulation (GDPR), public access to WHOIS data is increasingly limited. Indeed, access to domain Registrant data in WHOIS is, with limited exceptions, now very restricted. As discussed below, this exacerbates major cybersecurity, consumer safety, and commercial harms.

As you know, WHOIS data, which is comprised of the contact information provided by domain name registrants, including name, address, phone number, email address, and certain other attributes of a domain name registration, has been publicly accessible for free since the inception of the Domain Name System. Generic top-level domain name registrars and registries

are contractually required by ICANN to collect contact information from all domain name registrants at the time of registration. By default, the data is made publicly available for generic top-level domain spaces like .COM, as well as certain country-code domain spaces. This is like a "white pages" for domain names; it tells you who owns what on the internet. As the world becomes more interconnected, and information flows freely between different networks and over geographic boundaries, WHOIS data helps preserve the essential notion that the internet is a safe and secure place to do business.

The implications of limited access have serious consequences. WHOIS records are critical to the work of law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, copyright and trademark holders, journalists, academics, and others who rely on this information to help determine *who is* operating a criminal website, sending malicious (SPAM, phishing) emails, or initiating cyber attacks. NTIA correctly identifies a number of outcomes in its Request for Comment that underscore the importance of the WHOIS database for privacy implications - from Transparency (a user's ability to understand who they are communicating with), to Access and Control (a user's ability to have recourse to the domain name collecting, storing or displaying information), to Risk Management (a user's ability to *know* that the individual on the other side of the screen is who they say they are), all of these concepts are impacted by an open, accessible WHOIS database.

In the recently released ICANN GDPR and WHOIS Users Survey sponsored by the APWG and M3AAWG security organizations, author David Piscitello concludes from his analysis of over 300 responses from security practitioners:

> "We find that the changes to WHOIS access following ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data1 ('Temp Spec', adopted in May 2018), is significantly impeding cyber applications and forensic investigations and allowing more harm to victims. The policy has introduced delays to investigations and the reduced utility of public WHOIS data is a dire problem. Delays favor the attacker and criminal, who can claim victims or profit over longer windows of opportunity while investigators struggle to identify perpetrators or strip them of their assets (i.e., domain names) with limited or no access to the data that had previously been obtained or derived from WHOIS data. The loss of timely and repeatable access to complete WHOIS data is impeding investigations of all kinds, from cybercrime activities such as phishing and ransomware, to the distribution of fake news and subversive political influence campaigns."[1]

Comments by Steven Wilson, Head of the European Center for Cybercrime, at the recent ICANN meeting in Barcelona, underscore this point. He stressed that the GDPR has "created an unintended consequence for law enforcement and WHOIS and is now starting to impact

[1] https://www.m3aawg.org/sites/default/files/m3aawg-apwg-whois-user-survey-report-2018-10.pdf

significantly on law enforcement judicially and ultimately public safety."[2] Steven Wilson explained that WHOIS has been instrumental in everything from taking down an ISIS network to solving an investigation of a child abuse network, but both Europol and Interpol are now finding that investigations are being slowed down or hindered because of the lack of WHOIS records.

These challenges are not just limited to the EU. Only last month, at a hearing held by the Senate Caucus on the International Narcotics Control, Daniel Burke, Senior Operations Manager, Cybercrime Investigations Unit of the U.S. Food & Drug Administration testified that the lack of access to WHOIS data is impairing the FDA's efforts to combat the illegal online sales of opioids: "Conducting online investigations is not easy, and FDA has a narrow, but important role in combatting the online sale of opioids. For good or bad, much of the Internet ecosystem, including dark nets, have adapted and changed to build in anonymity. Public information about the owner of a domain name, known as "whois" data, is now often impossible to access with the implementation of the GDPR."[3] Many groups have been relying on historic WHOIS data that pre-dated GDPR, but as this data goes stale, more and more organizations and government agencies are being hindered in their investigative efforts.[4] When WHOIS data goes dark it takes away a critical source of information that is used to help keep the internet safe, secure and sustainable for all internet users.

CSTI encourages the Administration to do all you can to make WHOIS registration data publicly available 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. As discussed above, an open WHOIS database is critical to protecting consumers' online privacy, and as such we are requesting that a recommendation regarding WHOIS be included in the NTIA privacy principles.

We appreciate and thank you for your time and attention to this important issue. CSTI and our member organizations look forward to working with you in our efforts to ensure robust access to WHOIS data continues. Should you have any questions or concerns, please feel free to contact CSTI via Libby Baney (Libby.Baney@faegrebd.com) or Josh Andrews (Josh.Andrews@Faegrebd.com).

Sincerely,
The Coalition for a Secure and Transparent Internet
www.SecureandTransparent.org

[2] https://static.ptbl.co/static/attachments/191805/1540247405.pdf?1540247405
[3] https://www.drugcaucus.senate.gov/sites/default/files/FDA%20Testimony%20on%20Fentanyl%20final.pdf
[4] https://blog.domaintools.com/2018/09/whois-data-more-important-than-ever/