National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4701
Attn: Susan Chalmers
Washington, DC 20230

May 31, 2023

Re: Docket ID NTIA–2023–0006

Despite my initial intention to submit my own comprehensive feedback for the National Telecommunications and Information Administration's (NTIA) Request for Comments on the .US WHOIS, I am firmly convinced that the submission made by M3AAWG (https://www.m3aawg.org/sites/default/files/m3aawg_ntia_comments_.docx_.pdf) has already satisfactorily addressed all necessary points.

As stated in the M3AAWG filing:

“WhileM3AAWG understands and sympathizes with some of the legitimate concerns driving this proposed policy change, M3AAWG supports access to WHOIS data to the maximum extent possible to meet all legally permitted aims, including end users legitimate interests in avoiding spam, scams, abuse, and phishing as necessary and proportionate. In the absence of clear federal privacy legislation and in light of the importance of functional WHOIS for anti-abuse actors and end users, M3AAWG strongly supports unlimited, unencumbered access to .us WHOIS at this point and believes that more detail is needed to assess any proposal for change.”

"Based on our data and experience, most of the risk .us faces comes not from harvesting of WHOIS data, but from inadvertently creating conditions that enable abuse of .us domains for phishing, spam, scams and other online abuse and criminality. The availability of full .us domain registration data has positive impacts on domain abuse involving .us domains, as abusers tend to avoid public scrutiny enabled by data access. This “open source” model of policing has prevented .us from becoming known as a hotbed of abuse, as some other registries have. Having an open WHOIS that allows attribution leads to proactive mitigation efforts that stop abuse before it happens."

However, I am submitting for the record my opinion piece from September 2022 in response to the letter from Senator Wyden and other Members of Congress asking NTIA to make the .US WHOIS system go dark and put U.S. Cybersecurity & Consumer/Child Protection at risk. (https://medium.com/@rick.lane22/senate-letter-from-wyden-asks-ntia-to-undermine-u-s-cybersecurity-consumer-child-protection-f273d5ac50ed)

Sincerely,

Rick Lane
Child Safety Advocate

Senate Letter From Wyden Asks NTIA to Undermine ".US" Cybersecurity & Consumer/Child Protection

The Dark Whois/GDPR risk to cybersecurity, consumer privacy, and child protection is well documented by domestic and international law enforcement, cyber security experts, consumer protection agencies, child safety advocates, and intellectual property groups. But instead of Members of Congress "fixing" the Dark Whois/GDPR problem, Senators Wyden, Schatz, Warren, and House Members Lofgren, Eshoo, Khanna, Jacobs, Lieu, Malinowski, and Lynch sent a letter to the Department of Commerce National Telecommunications & Information Administration (NTIA) asking them to make the .US Whois database go dark. The letter justifies this request by stating, *"What is more, some of the largest domain registrars — handling tens of millions of domain registrations — receive on average fewer than 200 requests annually for previously-public registrant data from global law enforcement each year. This figure implies that public safety would not be significantly impacted by protecting the privacy of .US users."*

Besides the 200 number not being accurate, even if it was just 200 requests, these requests help prevent cybersecurity, phishing, malware, or ransomware attacks that could undermine U.S. national security and consumer and child protection.

How do I know? Because the FTC, Homeland Security, the FBI (ICANN 75 PSWG FBI presentation), and the FDA have all stated to Congress that a dark Whois harms U.S. citizens.

FTC Letter to Congress on Consumer Protection Investigations
"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.

The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants."

U.S. Homeland Security Criminal Investigations Letter to Congress
"HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI 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 criminals move their activity to a different domain."

FDA Letter to Congress Regarding Criminal Case Investigations
"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 (GDPR) has had a detrimental impact on FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients."

Here is another interesting quote from the letter that shows the complete lack of understanding of the threat of a Dark Whois. *"In fact, despite the domain industry increasing privacy protections*

for users over the last several years, the Internet Corporation for Assigned Names and Numbers (ICANN) has recently observed that the number of domains responsible for phishing, malware, spam, and botnets has declined."

Really?

Here is what a recent study from Cybercrime Information Center states:

Phishing Landscape 2022 Study
Phishing remains a significant threat to millions of Internet users. Phishing attacks lure victims to a website that appears to be run by a trusted entity, such as a bank or a merchant. The website, however, is a deception, and the site's content is designed to persuade a victim to provide sensitive information.
Among the major findings…
Over 1.1 million phishing attacks were identified, *a 61% increase over the May 2020 to April 2021 period.*

Malware Landscape 2022
Malware is a rapidly growing security threat. Malware can interfere with the operation of computer systems and networks; delete, suppress, or block access to data; and otherwise re-direct computing resources from legitimate to criminal purposes. Malware has become an organized criminal business and a weapons arsenal for cyber conflict and warfare. Financial losses, economic and political disruption, and harm to life and limb have turned malware into a priority global public concern.

Another quote from the letter states, *"The automatic public disclosure of users' personal information puts them at enhanced risk for becoming victims of identity theft, spamming, spoofing, doxxing, online harassment, and even physical harm…..In addition to putting users at risk of abuse of their information, the current lack of privacy protections chills vibrant expression and important speech online. Anonymity is a necessary component of the American right to free speech."*

So are the Members who signed the NTIA letter stating that since COPPA requires that the website operator's contact information — name, address, telephone number, and email address — must all be set forth publicly in the privacy policy, COPPA regulations violate the "free speech rights" of entities that operate websites targeted to children?
What about the Lobbying Disclosure Act (LDA), which requires individuals (exercising their 1st Amendment and Constitutional right to petition the government) to register with the Secretary of the Senate and Clerk of the House? Do these Members have the same privacy concerns for U.S. citizens whose information is publicly available on Congress's website? Maybe these Members would support an LDA "privacy proxy" regime.

But here is where the rubber meets the road and the real goal of the letter. The Wyden letter states, *"In addition to protecting users' privacy rights, directing these changes would also make .US a much more attractive space for domain registrations. For decades generic top-level domains have allowed customers to use privacy or proxy services to anonymize domain registrations. Indeed, many of the United States' largest trading partners' national domains offer privacy services and allow proxy registrations. Not only does publishing all .US user data risk harming users, it is simply bad for business."*

Whose business, GoDaddy's? .US is not a business, but a U.S. government-sanctioned country code top-level domain name (ccTLD). Why would we want a US government-sanctioned service to become a threat to US cyber security and consumer protection? So GoDaddy can sell more .US domain names. I hope that is not the outcome of this Wyden letter to NTIA. I hope this letter's ultimate outcome is to spotlight the fact that a Dark Whois (a threat to our national security, consumer protection, and child safety) is all about more money and less accountability for ICANN and its contracted parties.

Link to my opinion piece on ICANN's weak attempt to fix the gTLD dark Whois/GDPR problem: https://medium.com/@rick.lane22/horton-hears-a-whois-45a3db0113