VIA ELECTRONIC DELIVERY

Tuesday, May 30, 2023

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

Docket ID NTIA–2023–0006

Attn: Susan Chalmers,

The Alliance for Safe Online Pharmacies (ASOP Global) and The Partnership for Safe Medicines (PSM) are pleased to jointly submit the following comments for consideration to the National Telecommunication & Information Administration's request for comments on its proposal governing the access to the personal information of usTLD registrants.

Background

ASOP Global is a 501(c)(4) organization that seeks to protect patient safety globally and to ensure patient access to safe and legitimate online pharmacies in accordance with applicable laws. ASOP Global is active in the United States, Canada, Latin America, Europe, India and Asia. To learn more about ASOP Global, visit www.BuySafeRx.Pharmacy.

Comprised of more than 45 non-profit organizations, PSM is a public health group committed to the safety of prescription drugs and protecting consumers against counterfeit, substandard or otherwise unsafe medicines. To learn more about PSM, visit www.SafeMedicines.org.

1. In general, what are your views on the public availability of the usTLD domain name registration data to anonymous users? Has public access by anonymous users to usTLD registration data, especially personal information, resulted in exposing registrants to spam, phishing, doxing, identity theft and other online/offline harms? If such abuses have occurred, please provide illustrative examples. And, whether you are aware of examples of such abuse, do you believe that there is a significant risk of such abuse occurring in the future, if the current system remains unchanged (and if so, why)?

We believe that maintaining public access to usTLD domain name registration data is a vital and important aspect of maintaining and open, safe and transparent Internet experience for all. Public

accessibility of usTLD domain name registration data allows consumers to check who is behind domain names, allowing them to ascertain if the site is legit. Most importantly, it is a crucial tool for trademark rights holders to investigate website in potential violation of US trademark law. Finally, it is an essential and crucial tool for law enforcement to investigate and ultimately enforce against malicious registrants. Removing public access to usTLD domain name registration data would have the same chilling effect on consumer safety, trademark holder rights and law enforcement operations as did the EU GDPR rules. Allow us to explain:

Domain registration information, also known as WHOIS, has been a key tool in cybersecurity and consumer protection from the dawn of the modern Internet. Like public land and title information does for a store in a mall, it makes public *who is* behind a domain name or website. Importantly, WHOIS does not track who visits that domain in the same way a land or title record does not identify who visits a store. In the physical example, that is the standard that most consumers would expect when visiting a mall. In that way, those visiting a website should have some way to verify the online identify of the domain – at least against other online assets associated with that registrant; particularly when those websites are engaged in commercial activity (collecting or processing payments) or otherwise collecting information on the consumer.

Prior to the implementation of the European Union's General Data Protection Regulation (EU GDPR) temporary guidance in May of 2018, this information was readily available to law enforcement investigations, consumer protection, cybersecurity research, intellectual property rights protection and enforcement professionals. That temporary policy has become the standard now as ICANN has been unable to resolve the question of access to the satisfaction of many of the stakeholders – including the U.S. government. In response to Congressional inquiry, several federal agencies with enforcement responsibilities noted how the implementation of the EU GDPR has *negatively* impacted the ability to pursue cyber investigations and prosecutions.

Specifically:

- The **U.S. Food & Drug Administration** stated, "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 has had a detrimental impact of FDA's ability to pursue advisory and enforcement actions as well as civil and criminal relief in our efforts to protect consumers and patients."

- The **Federal Trade Commission** indicated, "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 **U.S. immigration and Customs Enforcement Homeland Security Investigations (HSI)** and the **National Intellectual Property Rights Coordination Center (IPR Center)** said, "HSI uses domain 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 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."

Congress, too, has weighed in on the question of access to domain registration information and included in the *Consolidated Appropriations Act for 2021* (P.L. 116-260) is report language that states as follows:

> "NTIA is directed, through its position within the Governmental Advisory Committee, to work with ICANN to expedite the establishment of a global access model that **provides law enforcement, intellectual property rights holders, and third parties with timely access to accurate domain name registration information for legitimate purposes**. NTIA is encouraged, as appropriate, to require registrars and registries based in the United State to collect and make public accurate domain name registration information."[1] (emphasis added)

For NTIA to propose a standard *less* than that to the .US space seems contrary to efforts to *increase* consumer protection.

We would remind NTIA of their prior work in support of domain registry transparency as well as enforcement against those who violate the law or domain name registry terms and conditions. As you may recall, ASOP Global and PSM supported the NTIA / FDA "trusted notifier" pilot program, which allowed a "trusted notifier" to provide credible and accurate information about illegal or abusive website content to domain name registries and/or registrars, including the .us domain registry. NTIA noted the pilot "yielded valuable insights into potential mechanisms to help in the fight against the opioid crisis." The pilot program made clear that NTIA believes that illegal drugs can be sold on websites hosted on the .us and other top-level domains and we encourage NTIA to take that into consideration.

The experience with the EU GDPR has given us the ability to see what would happen and we can use those experiences to inform us on any policy changes made to the .US space. In 2021 a survey was conducted by Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) to "determine the impact of ICANN's implementation of the EU GDPR." According to that survey: "From our analysis of 277 survey responses, we find that respondents report that changes to WHOIS access **continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattacks**."

In addition:

- 94% of respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors.
- Two-thirds of respondents indicate that their ability to detect malicious domains has decreased.

In summary, we strongly believe that applying similar restrictions around access to domain registration would result in similar trends in the .US space and have devastating, wide-ranging and potentially irreversible impacts on consumer safety, trademark holder rights and law enforcement operations.

[1] https://www.govinfo.gov/content/pkg/CREC-2020-12-21/pdf/CREC-2020-12-21-house-bk3.pdf

2. Do you believe the current system of anonymous access to usTLD domain name registration data should remain unchanged? If so, why?

Yes, we believe that for domains that are tracking or collecting user information, being used for commercial purposes (including the collecting or processing of payments), or otherwise capturing any information on consumers visiting their site, their domain registration information should be publicly available.

3. What legitimate purposes for access to usTLD domain name registration data should be included in the System's pre-defined list? Please provide a rationale for each category recommended.

Some baseline of information that establishes an online identity to the registrant behind a domain on .US should exist for any anonymous consumer to have the ability to due basic due diligence. This should be particularly true in instances utilizing the .US ccTLD as it implies a level of formality or relation to the federal government that could be misleading to consumers.

Additional levels of information should be available to IP & trademark rights holders to investigate potential IP rights violations by the site.

Lastly, full access to all data should be available for U.S. law enforcement for the purpose of investigations and enforcement actions.

4. Are there policies and practices developed or employed by other ccTLDs regarding WHOIS access that could be incorporated into the usTLD space? Please be specific in your response.

Yes. We encourage the NTIA to study Denmark's experience in this regard. In 2014, Denmark enacted legislation to require that the name, postal address, and phone number of all .dk registrants, with narrow exceptions, be publicly accessible. The accuracy of the data provided by registrants is also verified and a domain will not be issued if the data supplied is inaccurate or incomplete. As a result of these policies that emphasized transparency and accountability, the levels of abuse on .dk are among the lowest of any top-level domain.

5. Should the System distinguish between personal and non-personal registration data, and if so, how?

The System should collect standardized, accurate information. For business registrations for domains that are tracking or collecting user information, being used for commercial purposes (including the collecting or processing of payments) or otherwise capturing any information on consumers visiting their site, physical address (registrations to anonymous third party proxy addresses such as PO Boxes should be prohibited), telephone numbers and registering individuals should be publicly available to allow for Know Your Customer verifications, investigations and enforcement.
Registrations for person websites, do not necessarily need to include a physical address, telephone number or other overly specific personal information; however, it should include an email address as well as information surrounding the registrant and terms of registration to enable a consumer to identify it against other online assets as a way to verify its legitimacy.

6. Should usTLD registrants be notified when their data is accessed through the System? If so, why, when or in what circumstances?

ASOP and PSM have no strong opinion to this matter and believes its more appropriately addressed by those in law enforcement and enforcement, generally, as those efforts could impact potential investigations and/or prosecutions.

7. Under what circumstances, if any, should the Contractor require certain requestors to furnish a warrant when requesting access to usTLD registration data?

For domains that are tracking or collecting user information, being used for commercial purposes (including the collecting or processing of payments), or otherwise capturing any information on consumers visiting their site, a warrant should never be required. Any anonymous consumer should be able to access the basic registration information behind a website collecting information on them.

ASOP cannot identify any scenario where a consumer has *less* right to privacy than a website that is collecting information on the consumer.

8. The Contractor has proposed that the System provide special access to recognized and authenticated law enforcement and similar entities. Please provide feedback on this concept. If this proposal is adopted, how should it work? Are there best practices in other similar situations or other TLDs that could be used for such a special access portal? What steps should be taken, if any, to ensure the confidentiality of law enforcement requests through the System?

ASOP and PSM have no strong opinion to this matter, and we defer on the details to law enforcement, however we believe as stated above that a higher-level access to the full registration data for law enforcement will be crucial to aid in enforcement against IP and other law violations. Various law enforcement portals exist around the world, including a dedicated IP enforcement terminal from Europol, with a plethora of different layered access by investigation and clearance level. In general law enforcement is very skilled and experienced in routinely handling confidential information as part of investigations and have existing rules and processes to ensure the integrity of such confidentiality to not jeopardize any investigation or make evidence inadmissible in court proceedings. We have heard from law enforcement that access to bulk registration information is critical to connecting malicious networks and preventing further harm. We refer you to U.S. law enforcement for details.

In addition, third-party groups, academics, consumer advocates and, in fact, consumers themselves all assist in the identification and reporting of suspicious or fraudulent websites. Many enforcement agencies have portals that enable consumers to report activity deemed suspicious or fraudulent and encourage this level of engagement. The FTC has been one of those vocal on the role domain name registration plays in combatting fraudulent activity and, specifically, in empowering consumers to protect themselves. In its response to a Congressional inquiry in 2020, the FTC noted how the loss of access to this information, broadly, has limited the resources consumers could use to verify who is on the other side of the screen:

> "This lack of access also limits consumers' ability to identify bad actors using WHOIS information. **Prior to the GDPR, thousands of the complaints filed in our Consumer Sentinel compliant database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.**"[i] (emphasis added)

Enabling broader access to consumers serves as a 'force multiplier' for law enforcement who are combatting a never-ending number of websites and domains that criminal networks are able to register in seconds.

9. What entities in addition to law enforcement, if any, should have special access to usTLD registration data through an authenticated portal? Why?

Trademark & IP rights owners should have increased levels of access to websites suspected of U.S. IP law. This additional access could be granted on a case-by-case basis to allow for initial investigations by rights holders to support future law enforcement referrals and subsequent investigations. Europol's dedicated IP website is again a good example that allows rights holders to request and be granted enhanced access to enforcement actions involving their products.

As noted above, for domains that are tracking or collecting user information, being used for commercial purposes (including the collecting or processing of payments), or otherwise capturing any information on consumers visiting their site, their domain registration information should be publicly available. In those scenarios, any anonymous consumer should be entitled to at least as much privacy as a website; particularly those registered using .US.

10. What accountability and/or enforcement mechanisms should be put in place in the case of breach of the System's TOS by those that access the registration data?

It should be the requirement of the Contractor to ensure the requirements of the System are met. The Contractor can ensure this information is collected and maintained as they *must* have it to complete the financial transaction necessary to enable the use of the domain. In this way, the most critical part of implementing any system is *naturally* occurring. Enforcement can therefore be applied efficiently at the Contractor level.

11. Do you foresee any challenges to implementation of the System, or elements thereof, for example in distinguishing between personal and non-personal registration data, enforcement of System misuse, etc.? If so, how might these challenges be addressed?

ASOP believes that the proposed System overcomplicates the ultimate goal of protecting consumers. Open, accessible domain registration information had been publicly available since the dawn of the modern Internet. It did then, and still does today, play a critical role in protecting consumers by providing enabling them to do a basic level of due diligence before engaging with a website.

NTIA should focus its efforts on identifying the aspects of WHOIS information that should *not* be made public and maintain a baseline level of information that at least enables consumers and other

stakeholders to be able to identify *who is* behind a domain at least to the level of connecting it to other online assets as a way to verify its identify.

12. Should the Accountable WHOIS Gateway System be offered as an opt-in or opt-out service for current and new usTLD domain name registrants?

ASOP believes that for any domains that are tracking or collecting user information, being used for commercial purposes (including the collecting or processing of payments), or otherwise capturing any information on consumers visiting their site, their domain registration information should be publicly available. For other domains it should be offered as an opt-out.

Conclusion

We welcome the opportunity to further engage with NTIA on this important matter. Please contact Elliot Vice with ASOP Global at elliot.vice@faegredrinker.com if we can provide further assistance. Thank you for your

[i] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/