In re: Introduction of Accountable Measures Regarding Access to Personal Information of .us Registrants RIN 0660–XC058 May 31, 2023	)	Comments of The Coalition for Online Accountability ("COA")

J. Matthew Williams
Mitchell Silberberg & Knupp LLP
1818 N St. NW, 7th Floor
Washington, DC 20036
mxw@msk.com
202-355-7900
Executive Director for and Legal Counsel to COA

The Coalition for Online Accountability ("COA")[1] is pleased to submit these comments to The National Telecommunications and Information Administration ("NTIA"). COA is a longstanding group of companies, trade associations, and copyright member organizations dedicated to enhancing and strengthening online transparency and accountability. To support its mission COA is working to ensure that domain name and IP address WHOIS databases remain publicly accessible, accurate, and reliable, as key tools against online infringement of copyright, as well as to combat a variety of illegal (and often anonymous) acts, including, cybersquatting, phishing, trademark infringement, cyber-crimes and other unlawful activity online. There is no doubt that the motion picture, music and video game industries, as well as their consumers, have long suffered from widespread online piracy and other abuses. Increasing, not decreasing, the tools that should help to thwart such conduct is of great importance to COA's members and the public at large. In these comments, we focus on the issues of most relevance and significance to our coalition and industries. We thank NTIA for considering our input.

[1] COA comprises Broadcast Music, Inc. ("BMI"), Entertainment Software Association ("ESA"), Motion Picture Association, Inc. ("MPA"), NBCUniversal, Recording Industry Association of America, Inc. ("RIAA"), The Walt Disney Co., and Warner Bros. Discovery.

INTRODUCTION

In the Request for Comments ("RFC"), "NTIA seeks public comments regarding the proposed Accountable WHOIS Gateway System (System)." However, the RFC provides only vague information about this "proposed" System. There is no copy of any actual proposal from GoDaddy attached to or referenced in the RFC. To our knowledge, there is no publicly available copy of any written proposal for this System.[2] All we have been able to locate online is a vague 2022 PowerPoint presentation prepared by GoDaddy. While there may be more information available online, the public should not have to go looking for it to respond to the RFC and our ability to respond fully is hampered without access to that information.

The RFC states that NTIA is considering adopting this ethereal System "[i]n response to concerns about the potential for abuse of usTLD registrant data." Yet, the RFC provides no details about any specific concerns being raised with NTIA. Instead, the RFC simply cites in a footnote to one, subjective, opinion piece by Andrew Alleman published in April 2022 on the author's own website, Domain Name Wire. In the piece, Mr. Alleman identifies one situation that caused "public outcry." He does not provide any other evidence that anyone is abusing registrant data acquired through the .us WHOIS process.[3] The RFC's footnote also states that GoDaddy "has also received a number of complaints outlining these issues." To pattern, the RFC includes no details regarding these alleged complaints either. The RFC does not provide the number of these alleged complaints received by GoDaddy; their nature; their substance; their accuracy/credibility; or whether GoDaddy provided the alleged complaints to NTIA. Perhaps that is why the RFC refers to "the *potential* for abuse" rather than stating that abuses have occurred. The lack of such details, like the lack of details regarding the proposed System, makes the task of responding to the Request for Comments challenging. Nonetheless, any such abuses could only pale in comparison to the rampant illegal activity online, and the ability to address that illegal activity will be significantly hampered by limiting access to .us WHOIS data

If additional details concerning the proposed System or the alleged complaints become a part of the record through comments submitted in response to the RFC, COA asks that NTIA issue a

---

[2] COA appreciates that the RFC states: "Under this proposal privacy and proxy services would remain prohibited under the usTLD as currently required by the .us contract." This is critically important to COA's members.

[3] He does reference changes made by other registries and registrars resulting from the European Union's General Data Protection Regulation ("GDPR"). However, many of these changes were never justified under GDPR in the first place. The E.U.'s new Network and Information Security Directive ("NIS2") now makes that clear while also imposing specific requirements on registries and registrars to provide access to registrant data. *See* Dean Marks, *NIS2, ICANN and "Thick" WHOIS: A Mandate to Move Forward*, CIRCLEID, Jan. 11, 2023, https://circleid.com/posts/20230111-nis2-icann-and-thick-whois-a-mandate-to-move-forward

request for reply comments in order to prevent members of the public who are not yet behind the proverbial curtain to address an actual, written proposal for a System designed to prevent actual, identified abuses of WHOIS.

With that said, COA understands that NTIA did receive, in September 2022, a letter from Members of Congress[4] expressing privacy concerns related to the .usTLD and WHOIS. While that letter also lacks details concerning identified WHOIS abuses, COA, of course, takes the concerns of these Members of Congress seriously. COA also understands that NTIA, in December 2022, received a letter on these issues from Members Latta and Schakowsky,[5] detailing why maintaining an open WHOIS system for the .usTLD is so crucial to American interests, including those of intellectual property owners, such as COA's members. The letter explained that a lack of open access to accurate, verified registrant data actually harms, rather than helps, members of the public. It also described the relevant policy-making background and stressed that Congress has not yet passed federal privacy legislation, which should give NTIA pause before proceeding with altering the current .usTLD WHOIS system. COA strongly endorses the content of that letter.

In summary, from the point of view of intellectual property owners, our comments will address – as best we can in light of the above-stated omissions in the RFC itself – the questions raised by the RFC.

RESPONSES TO RFC QUESTIONS

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, doxxing, identity theft and other online/offline harms? If such abuses have occurred, please provide illustrative examples. And, whether or not 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)?

COA members, to their knowledge, have not been harmed by the public availability of the .usTLD domain name registration to anonymous users of WHOIS.[6] We do not believe that there

[4] https://www.wyden.senate.gov/news/press-releases/wyden-eshoo-lead-bicameral-effort-urging-ntia-to-protect-website-owners-personal-information-quickly-adopt-strong-privacy-protections-

[5] https://secureandtransparent.org/wp-content/uploads/2022/12/12.14.22-Letterhead-NTIA-US-WHOIS-Latta-Schakowsky.pdf

[6] COA stresses that "personal information" should not be understood to encompass the names and contact information of legal entities as opposed to natural persons. Even if .us was subject

is a significant risk of such abuse occurring in the future. Instead, the risks presented by modifying the current system, which we discuss further below, far outweigh the risks identified in the question. When other TLDs impose restrictions on access to registrant data, that empowers bad actors who engage in disseminating spam, phishing, doxxing, identity theft and other online/offline harms.

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

Yes. As stated in the RFC, "[h]istorically, NTIA has authorized public access to the usTLD registration data (WHOIS service) permitting internet users to retrieve the usTLD registrant data for legitimate purposes (e.g., law enforcement investigations, consumer protection, cybersecurity research, intellectual property rights protection and enforcement)." The RFC includes no particulars to explain why that unencumbered accessibility, especially for the identified purposes, should be eliminated. No federal privacy legislation has passed to justify altering the current system in any way. Statistics already indicate that .usTLD registrants themselves engage in significantly *more* abuses of the DNS than registrants using other ccTLDs, such as .uk, .au, and .de.[7] Privacy is important, but these statistics indicate NTIA and GoDaddy should be more focused on preventing abuses, including privacy abuses, by .us registrants than on creating more barriers to access registrant data.

We also refer to our above answer to question 1.

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

The RFC states:

> The System would require those seeking access to the usTLD registration data to provide their name, an email address, and to accept the Terms of Service (TOS). The TOS would require the user to agree not to misuse the data. Users would also be required to identify, from a pre-selected list, a legitimate, non-marketing purpose for accessing the information. This list would be developed according to industry best practice in consultation with the usTLD community and approved by NTIA. Unredacted WHOIS data would then automatically be returned in near-real-time to the user via email. Queries would be rejected only if the user did not

---

to the GDPR, which it is not, NIS2 makes clear that legal entities are not protected by GDPR and registrant data about such entities should be easily accessible. *See* note 3, above.

[7] https://www.spamhaus.org/statistics/tlds/ (the statistics are subject to change on a daily basis).

provide a name and email address or failed to select (or provide) a legitimate purpose and accept the TOS.

First, COA opposes the adoption of the proposed, nebulous System. However, if NTIA adopts a new system, COA strongly encourages NTIA to include intellectual property owners, as well as, but not limited to, their agents, attorneys, investigators, trade associations, and licensees, in a predefined list of authorized requesters, to aid them in combatting illegal activity online. No proof of copyright or trademark ownership should be required.[8]

Second, the notion that data requesters must agree to a one-sided, take-it-or-leave-it, TOS agreement is very troubling. We oppose it. To our knowledge, NTIA and GoDaddy have not provided the language for any such agreement, including without limitation how "misuse" of data would be defined; what penalties would be imposed for alleged violations of the TOS; and whether the TOS would include inappropriate waivers of claims.

We also refer to our above responses to questions 1 and 2.

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.

COA opposes the adoption of the proposed System and believes the current system should remain in place. While the policies and practices of some other countries could be useful if NTIA adopts a new system, at this time we agree with the sentiments expressed by Members Latta and Schakowsky in their December 2022 letter. U.S. policy, not the policies of other nations, should dictate how .us is operated.

We also refer to our answers above to the first three questions.

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

Again, COA opposes the adoption of the proposed System. It is important to note, however, that legal persons/entities should *not* be considered to be providing "personal registration data" when acquiring a .us registration. Please see footnote 3, above.

[8] The RFC states: "The System would also permit users to identify a legitimate purpose outside of the pre-selected list. The Contractor using usTLD community developed and NTIA approved standards would manually review these requests and deliver, via email, unredacted data within two (2) business days for any non-abusive purpose unrelated to marketing. The System would also provide a mechanism to expedite emergency requests." Assuming NTIA adopts a new system, which it should not, expedited access for requesters who somehow fall outside the "pre-selected list" would be crucial and the contract should not provide GoDaddy with much leeway to determine who gets expedited access and who does not.

Also, the RFC states: "Non-personal information relating to the domain name would remain available for retrieval via anonymous query. This information includes domain name and ID, registrar WHOIS server, registrar URL, updated date, creation date, registry expiry date, registrar, registrar IANA ID, and registrar abuse contact (email and phone number)." It should go without saying that if NTIA adopts a new system, such data should continue to be provided in response to all requests. However, that data alone is insufficient to assist in combatting illegal activity online.

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

No.

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

None.

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?

The RFC states:

> To address the unique needs of law enforcement and other similarly situated entities, the Contractor would establish a portal for authenticated law enforcement users, which would grant such users near real-time access to personal information. The Contractor would continue to work with law enforcement authorities and others to ensure that investigatory confidentiality and unique other needs with respect to access and confidentiality are fully met.

We reference our above response to question 3. If NTIA adopts a new system, however, COA strongly supports a portal for law enforcement and similar entities to obtain real-time access to personal information. Several U.S. authorities/agencies have publicly stated they frequently encounter problems with systems that do not provide such access. COA also believes that IP rightsholder trade associations and other organizations that protect the interests of copyright and trademark owners should be considered "similarly situated entities" given their constant need to access registrant data to identify, investigate, verify, and thwart, through legal action or other means, infringement. There are likely other organizations that should have access to the portal. Without more information about the proposed System, COA cannot at this time provide suggestions for how the portal should work or how "similarly situated entities" should be identified.

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

We address this question in our above answer to question 8. We stress here that organizations that represent the interests of intellectual property owners confront infringements and other online, illegal activity on a daily basis, including by large-scale piracy enterprises, cybersquatting, phishing and other scams. Impeding or slowing investigators down through unnecessary hurdles hurts not only America's creative sector, but consumers as well. Many infringers use their websites to scam, phish, spam, and otherwise invade unwitting consumers' privacy and financial data.

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?

Please refer to our response to question 3. Requesters should not have to agree to a TOS to access registrant data. If NTIA and GoDaddy publish a proposed TOS, COA would likely be able to provide more specific responses to the RFC's questions, including this one.

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?

We incorporate by reference all of our other answers. Also, it is COA's view that the adoption of any new system would create vulnerabilities enabling bad actors to take advantage of the system. That is the very essence of their businesses – figuring out how to hide from exposure and punishment for DNS abuses[9] by exploiting policies and practices that may be enacted with good intent but nevertheless allow for malicious DNS users' "anonymity."

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?

COA opposes the adoption of a new system. If NTIA nevertheless adopts one, the default setting should be that all registrants' data remains openly accessible.

CONCLUSION

COA appreciates the opportunity to provide NTIA with these comments on the status of WHOIS within the .usTLD. However, the RFC lacks sufficient detail and data on the "proposal" at issue. And, more importantly, NTIA should maintain the current system, which has worked well and reflects current U.S. policy.

[9] COA supports the approach to defining DNS Abuse taken in the E.U.'s January 2022 Study on Domain Name System ("DNS") abuse: https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1