COMMENT OF THE ICANN BUSINESS CONSTITUENCY
Submitted by email to usTLD@ntia.gov on May 31, 2023

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration (NTIA)

[Docket Number: 230412–0099]

RIN 0660–XC058

Introduction of Accountable Measures Regarding Access to Personal Information of .us Registrants

---

The Business Constituency (BC) is the representative voice of business users of the internet and their customers as their concerns relate to governance of the domain name system (DNS). Our constituency is chartered by the Internet Corporation for Assigned Names and Numbers (ICANN), the multistakeholder body charged with maintaining a secure and stable DNS.

The BC, over time, has carefully considered all aspects of the debate over domain name registration data (or "WHOIS") policy as it has progressed. While sensitive to the concerns raised in this proposed policy change for the .US country code top-level domain (ccTLD), the BC in this comment lodges again its position that WHOIS data must be accessible to the broadest extent possible. In our experience, access to an unencumbered WHOIS database is beneficial to the public interest and helps insulate against a rising tide of DNS abuse.

Our replies to the specific questions posed in the Request for Comment follow herein. Thank you for the opportunity to comment.

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)?

Our view on the public availability of usTLD domain name registration data mirrors that of our stated previous positions regarding registration data (or "WHOIS") availability in any TLD: That access to a complete, accurate and verified WHOIS database is warranted and should not be undermined or otherwise artificially restricted.

There exists significant risk in closing yet another namespace. While anecdotal evidence may exist regarding the potential harms identified in the question above, there is significant, well-established and ongoing research documenting that:

- Abuse of the domain name system (DNS) and related infrastructures -- including phishing, malware, pharming, impersonation and other harms -- has, over time, become a rapidly growing problem; and
- WHOIS is a key investigatory tool for pursuing accountability relating to criminal or abusive behavior.

Thus, our position, which has not changed, is that WHOIS is a public interest tool that should be made available as efficiently as possible.

It must be pointed out as well that the criticality of accurate and accessible WHOIS data is consistently and well articulated by the US government itself, both over time and, further, recently.

In 2006, when WHOIS-related policy development began to mature, the Federal Trade Commission established its position as solidly in favor of an open and accurate WHOIS database. To quote then-Commissioner Jon Liebowitz:

> ***The FTC believes that the Whois databases, despite their limitations, are nevertheless critical to the agency's consumer protection mission, to other law enforcement agencies around the world, and to consumers.*** *The use of these databases to protect consumers is at risk as a result of the Generic Names Supporting Organization's ("GNSO") recent vote to define the purpose of Whois data as technical only. The FTC is concerned that any attempt to limit Whois to this narrow purpose will put its ability to protect consumers and their privacy in peril.* (Emphasis added)
>
> and:
>
> *FTC investigators and attorneys have used Whois databases for the past decade in multiple Internet investigations. Whois databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed,* ***it is difficult to overstate the importance of quickly accessible Whois data to FTC investigations.*** (Emphasis added)

Further to the FTC's interest in WHOIS policy, in comments raised in reply to the FTC's proposed Trade Regulation Rule on Impersonation of Government and Businesses, commentors were clear in their advocacy of an open WHOIS database as a means of combating impersonations of businesses and governments.

In addition to FTC concerns regarding WHOIS availability, in its July 2022 letter to ICANN, the Food and Drug Administration expressed its frustration with the accessibility of WHOIS as it relates to enforcement capability. The letter reads, in part:

> *"…since personal contact information within WHOIS records became unavailable to U.S. investigators under ICANN's implementation of the European General Data Protection Regulation (GDPR) in 2018, the issue regarding WHOIS access for public health and law enforcement agencies is still unresolved some four years later."*

Even the NTIA, the agency now proposing further WHOIS restriction, articulated its then-position about the importance of the availability of WHOIS access, in the context of its participation in ICANN's Governmental Advisory Committee (GAC) discussions on WHOIS. See:

> NTIA statement to the GAC, March 13, 2018:
>
> *"…I just wanted to provide some views from the United States with respect to the GDPR and how WHOIS is going to be dealt with in light of that as well as what ICANN has asked of the GAC, so if that's a good time I'm happy to carry on. So,* ***from the U.S. perspective maintaining access to WHOIS is very important.****"* (Emphasis added)
>
> NTIA statement to the GAC, March 10, 2019 (*after* the imposition of the European Union's General Data Protection Regulation (GDPR)):
>
> *"…****we strongly believe there's a lot of urgency to making sure there are predictable, efficient ways in which to request and get access to redacted information.****"* (Emphasis added)

In summary, our position mirrors the position historically articulated by NTIA itself, as well as other governmental authorities with a stake in a safe internet namespace: that an accessible WHOIS database that permits investigatory efforts is more likely to prevent DNS abuse than it is to enable other types of harm.

We respectfully refer NTIA to the expert report[1] by the Anti-Phishing Working Group (APWG) and the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) regarding the negative outcomes of WHOIS redaction by other top-level domain registries, which we believe underlines our comment.

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

Yes. Simply put, the public interest role of domain name registration data should not be ignored, particularly in light of the quickly rising threats facing Americans at home and abroad because of DNS and other types of abuse and online harm.

If the system being proposed would hamper the immediate investigatory efforts of cybersecurity authorities, intellectual property rights holders, law enforcement and others, it proffers more harm than good. While further detail about the NTIA proposal may warranted, our informed opinion -- following now nearly five years of experience with a darkened WHOIS database -- is that limitations of WHOIS availability drive up abuse in associated namespaces. (Please refer again to the 2021 M3AAWG WHOIS study for further detail about *demonstrated* difficulties produced by strictly limited access to WHOIS.)

Our recommendation, which mirrors that of others, is that the NTIA examine, contemporaneously, the level of abuse in the .US namespace as it correlates to WHOIS records and the potential impact of closing the .US WHOIS system in terms of propagating DNS abuse. Stakeholders on both sides of the issue should be properly heard, with equal bearing given to those who utilize WHOIS records to advance the public interest and the security and stability of the DNS. Re-evaluation of this proposal would be better informed following such research to ensure either that the proposal's objectives would be met or, more likely, whether unintended consequences would arise as a result.

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.

More information is necessary regarding the proposed email system in order to knowledgeably answer this question. As industry colleagues point out, auditing and enforcement capabilities would be required for the authentication and identity verification measures necessary to a correctly functioning system.

However, we point out a wide range of functions that might be included in a predefined list, should the NTIA insist on forging ahead with the proposal. This non-exhaustive list includes consumer protection (consumers confirming the identities of those with whom they do business); law enforcement (investigating online harms, including purveyors of child sexual abuse material, and prosecuting offenders); intellectual property and brand protection (prevention of impersonation, infringement and theft); cybersecurity research (prevention or mitigation of rapidly scaling cyberattacks); and the prevention or mitigation of known forms of DNS abuse, including malware, phishing, spam, botnets, and other forms of harm.

We further respectfully suggest that instead of a cumbersome system that burdens the requestor with a demand for justification of access requests, which then would presumably be reviewed case-by-case, any .US WHOIS policy should list the purposes that are expressly disallowed (e.g., data harvesting or marketing). This would make the system not only open to the appropriate users, but far more efficient in dealing with access requests. The policy should also clarify that for the pre-approved purposes, the response is real-time, with no ability for the .US contractor to challenge the request or delay the disclosure.

[1] "ICANN, GDPR and WHOIS Users Survey" http://www.m3aawg.org/WhoisSurvey2018-10 and "ICANN, GDPR, and the WHOIS: A Users Survey - Three Years Later" https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

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. It is known, and has been known for some time, that various ccTLD policies and practices have taken an intelligent approach to WHOIS administration, resulting in appropriately open access without a rise in abuse of the database.

The best-known example is that of .DK, the ccTLD of Denmark, which requires the publication of certain WHOIS data fields. The .DK registry requires accuracy and -- importantly -- verification, which has resulted in a drastically lower rate of DNS abuse. Emphasizing accuracy and verification would do more to ensure the integrity of .US WHOIS, yielding lower abuse levels, than would the artificial restriction of registration records.

We note that the proposal only addresses one aspect of WHOIS – the requester side – without addressing the accountability that is associated with a verified, more accurate WHOIS from the registrant. ccTLDs typically see less abuse when they have a more robust, accurate WHOIS policy, since bad actors seek to avoid detection.

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

This question suggests a registry or registrar should treat a registrant's data differently depending on whether that registrant is a legal or natural person, an outcome not dictated by current US privacy regulation.

Our input is that .US WHOIS records should remain transparent until U.S. national privacy legislation is adopted that pertains specifically to the WHOIS database. Note further that legal persons -- such as corporate entities -- are not protected by privacy law in the same way natural persons are. Accordingly, there is little reason to hide data from legal persons.

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

The question assumes the implementation of the system as proposed by NTIA. We reiterate here that we believe such a system is unnecessary and potentially harmful. However, to the specifics of the question, were the system to advance, we believe notification is unnecessary -- and could be potentially damaging, even -- as an across-the-board practice.

For example, notification to a nefarious registrant of access to his/her WHOIS data could be an unintentional signal that that registrant is under investigation by law enforcement or cybersecurity authorities.

Accordingly, we believe a notification system is more likely to be unworkable than it would be beneficial.

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

If the WHOIS database remains liberally available, as we so advocate, the provision of a warrant will be generally unnecessary to retrieve registration data. A warrant may be helpful, however, in cases where additional customer information (e.g., payment data, other usTLD domains registered by the customer) would be useful to investigators.

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?

We respectfully point out here that law enforcement agencies (LEAs) represent the *minority* in the ongoing effort to prevent or mitigate DNS abuse. Most of this effort is headed by others (e.g., registries, registrars, ISPs, cybersecurity experts, brand holders, and even private individuals). LEAs and others rely on one another for cooperation in investigatory and mitigation work; limiting access to LEAs only would effectively blind access for others and cause more harm than good.

Further, as has been indicated elsewhere, recognition and authentication of LEAs may be more involved than it appears. In the United States jurisdiction, LEAs may be more easily identifiable, but this is more unlikely across borders (where US LEAs rely on inter-agency collaboration). In addition, investigators are not always sworn law enforcement officers.

We repeat here that the ultimate answer -- rather than "picking and choosing" who gets access and who doesn't -- is to have an appropriately accessible WHOIS system for the .US namespace. Spotty and inconsistent access rules will not significantly combat rising DNS abuse rates, nor will it protect consumers and end users.

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

As noted in question (8) above, most abuse prevention and mitigation work is done by private organizations, not LEAs (though they sometimes work in concert). In our experience, it is highly unlikely that LEAs could assume full responsibility for all online investigatory work.

The productive answer to this question is to maintain an appropriately open WHOIS database; again, picking and choosing those authorized for access will invariably leave out the many who are equipped to deal with rising abuse rates.

We must also point out here the issue of scalability. Requests for record-by-record data (replies for which already are delayed or ignored by gTLD registries and registrars) represent the oft-cited "whack-a-mole" problem. An open WHOIS database allows much faster investigation and tracking of criminals at the "account" level, enabling the takedown of bad actor networks in a broader swath, rather than allowing those criminals to carry out their activity elsewhere after only one or a few problematic domain names are addressed.

Finally, NTIA must give heed to international law enforcement and other authorities, not just LEAs in the US jurisdiction. Even as the .US ccTLD requires a United States nexus, bad actors still use the .US namespace within and outside US borders to conduct their work. As such, international authorities deserve equivalency with their US colleagues.

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?

This is a difficult proposition as, in practicality, email-based identifiers may be quickly adopted and then abandoned for a replacement (or multiple replacements), negating action against TOS breaches by the original offender. Again here, scalability in enforcement efforts would be a nearly insurmountable challenge.

Our theme in replying to these questions is that an open and accessible WHOIS database is preferable to and more workable than one with what might be seen or experienced as ineffective roadblocks. Negative impacts of such a system have not been widely observed.

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?

Please see answers to the questions above regarding challenges to not only implementation of the proposed system, but in its practical use.

Generally speaking, the use of an email access system is unsuitable for current-day use; it is subject to error, further disregard by registries and registrars, and is too ill-defined in this proposal for practical consideration.

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?

Registrants intending to use .US domain names for abusive purposes will have no incentive to opt in to the publication or disclosure of their data. Therefore, an opt-in model is not advisable.

Submitted by email to usTLD@ntia.gov on May 31, 2023

Mason Cole
Chair
ICANN Business Constituency
mcole@perkinscoie.com
+1-503-407-2555

Steve DelBianco
Vice Chair for Policy Coordination
ICANN Business Constituency
sdelbianco@netchoice.org
+1-703-615-6206