July 11, 2022

The Honorable Robert M. Califf, MD
Commissioner
Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

Commissioner Califf:

On behalf of the Coalition for a Secure & Transparent Internet (CSTI), we are writing in response to the letter dated 14 June 2022 submitted to your agency from Goran Marby, President & CEO for the Internet Corporation for Assigned Names and Numbers (ICANN), regarding the recent presentation by Dan Burke on the topic of WHOIS information.

CSTI is a coalition of stakeholders with different policy focuses who came together over their concerns around the loss of access to WHOIS information because of an overly broad interpretation and misguided application of the European Union's General Data Protection Regulation (GDPR) by ICANN. Since 2018, CSTI has been educating lawmakers and others as to the historical importance of WHOIS information in protecting consumers online and how ICANN's policy has undermined America's national security, consumer protection, and online accountability due to its rendering useful WHOIS information essentially unavailable.

We appreciate Dan Burke's participation in our recent virtual briefing entitled, "*The Threat of a Dark WHOIS: Putting Americans' Health, Safety and Cybersecurity at Risk*." The intention of this program was to hear from professionals about their first-hand experiences with WHOIS to understand the impact that lack of access to this information is having on protecting consumers online, as well as with respect to our cyber and national security. Mr. Burke joined former law enforcement officials, cyber security professionals and other experts in the field of Internet law and policy in speaking about the issue and what they have experienced firsthand. In addition, two prominent Members of Congress submitted video statements regarding their interests and concerns over the WHOIS issue.

In his letter Mr. Marby indicates that, without proper context, Mr. Burke's presentation could be 'misleading.' CSTI takes issue with this characterization and believes Mr. Burke's long experience working in cyber investigations warrants attention to what he has witnessed. In addition, Mr. Burke's comments were in line with those of other presenters and countless other stakeholders and interested parties whose work to combat online illegal behavior has been severely impeded by the lack of ready availability of WHOIS information. The following are direct responses to the issues raised by Mr. Marby. As part of those responses, we are enclosing several documents with this letter for your review that demonstrate the strong concerns raised by several federal agencies around WHOIS.

Concern: A requester must have a subpoena to access non-public registration data

Mr. Marby indicates that, "it is not necessary to obtain a subpoena to gain access to non-public domain name registration data." NameCheap, which is the 2nd largest domain name registrar in the world with over 14 million domain names, clearly states on its own website:

> "We would like to call to your attention that we will not be able to provide you with any contact information of the domain name holder without expressed permission from the customer, **except under limited circumstances such as an official U.S. Court Order or Subpoena." (emphasis added)**

For entities without subpoena power, this can be the end of a cyber investigation.

Other registrars and registries have similar policies. As noted in an article by CircleID entitled, *"Retrospective: Post-GDPR Compliance Rates for Domain Enforcement"*:

> "The Temporary Specifications allows ICANN and gTLD registry operators and registrars to continue to comply with GDPR while still maintaining the existing WHOIS system to the greatest extent possible by restricting personal data to a layered/tiered access system. Unfortunately, participating registrars can make individual decisions about which requests to honor and which to deny. In addition, each registrar is able to set their own specific steps that need to be fulfilled when requesting personal information, leading to a diverse set of requirements that can range from filling out a simple online form **all the way up to requiring a legal subpoena."**[1]

Ultimately, responding to a WHOIS request comes down to the discretion of the registry or registrar in question, despite contractual obligations to collect and maintain this information. It is a subpoena that *compels* a registry or registrar to respond to the request at all. Given the time constraints around cyber investigations and the number of domain names that can be registered by criminal enterprises, WHOIS has become largely ineffective.

Further, Mr. Marby acknowledges in his letter that, "prior to the adoption of the European Union's General Data Protection Regulation (GDPR), registrars *were* required to publish WHOIS data, including registrants' personal contact information" and that, as a result of the GDPR, registrars must, "restrict publication of personal data for registrations with a nexus to the European Economic Area…[and for] registrations without an EEA nexus, registries and registrars may choose not to publish personal data on a global basis."

What Mr. Marby fails to acknowledge is that under ICANN's policy registries and registrars may choose not to publish on a global basis the WHOIS data of legal person registrants whose data is not considered personal data under the GDPR. This irresponsible policy decision on the part of ICANN has no basis or justification under the GDPR and has resulted in far more WHOIS data

[1] Retrospective: Post-GDPR Compliance Rates for Domain Enforcement (circleid.com)

being non-publicly accessible than would ever possibly be required under the GDPR. Consider the 2021 study conducted by Interisle which analyzed the effects of ICANN policy for WHOIS access, which found that:

- ICANN's policy has allowed registrars and registry operators to hide much more contact data than is required by the GDPR—perhaps five times as much.

- Including "proxy-protected" domains, for which the identity of the domain owner is deliberately concealed, **86.5% of registrants can no longer be identified via WHOIS—up from 24% before the ICANN policy went into effect**.[2]

Mr. Burke in his presentation acknowledged that some registrars are cooperative and therefore it is accurate that a subpoena or court order is not *always* necessary to gain access to non-public WHOIS data. However, Mr. Marby's statement that "Law enforcement and consumer protection agencies around the globe have relied on existing ICANN WHOIS policies to gain access to this data" is grossly inaccurate and misleading. Indeed, law enforcement and consumer protection agencies around the world have indicated that due to lack of access under ICANN's current policy, WHOIS data no longer meets investigative needs. A survey conducted by the Public Safety Working Group of the Governmental Advisory Committee to the ICANN Board of Directors of over 50 law enforcement agencies from around the world detailed how the lack of availability of WHOIS data since ICANN's implementation of the GDPR has interfered with the work of such government agencies. Prior to the adoption of the ICANN policy in May 2018, only 2% of the law enforcement agencies reported that WHOIS data did not meet investigative needs. Following implementation of the policy, **67% of the agencies reported that WHOIS data did not meet investigative needs.**[3]

In addition, a summary of response rates was produced by two leading enforcement vendors and one law firm in 2021. That summary covered 10,641 WHOIS requests with 4,075 proxy requests and found that:

- 93% of WHOIS requests to registrars and thick registries were not fulfilled - for an aggregate of 7% success rates. This continues the downward trend seen over the last year representing a significant decrease from the 20% success rate from ICANN 69 in October 2020.

- Approximately 21% of all WHOIS requests result in no response at all.

- Phishing-related requests or requests concerning obviously fraudulent domains are rarely fulfilled even for signatories of the Domain Abuse Framework.

---

[2] "In new study Interisle Reveals Excessive Withholding of Internet WHOIS Data" https://www.securityskeptic.com/2021/01/in-new-study-interisle-reveals-excessive-withholding-of-internet-whois-data.html. January 2021.

[3] https://gac.icann.org/presentations/public/icann63%20pswg.pdf

- When phishers register domains, they tend to use them quickly – more than half within 48 hours.

- With compliant WHOIS reveal requests taking an average of 7 days, the data often comes too late to protect the public from fraud.

- The delays and roadblocks in WHOIS are a boon to attackers and criminals, prolonging their windows of opportunity to cause harm during cybercrime activities.

- One major registrar has introduced significant fees for legitimate requests to redacted WHOIS, raising ICANN compliance concerns.[4]

With respect to U.S. government agencies, Congressman Latta (R-OH) sent letters to several Executive branch agencies in 2020 to better understand their experiences with WHOIS information prior to and since, the implementation of the EU GDPR. Copies of those letters are enclosed. Consider:

- The FDA indicated that, "FDA cannot access WHOIS information without a Grand Jury subpoena," and, "FDA's Office of Criminal Investigations (OCI) does not have authority to issue an administrative subpoena for basic WHOIS data or WHOIS data shielded by a privacy / proxy service."

- The Federal Trade Commission (FTC) expressed similar frustration in its response stating, "before the GDPR went into effect, the FTC could quickly and easily obtain detailed information about the name, address, telephone number and email of the domain name registrant by typing a simple query. Since May 2018, however, we generally must request this information directly from the particular registrar involved."

- The U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) indicated in their response to Rep. Latta dated July 16, 2020:

> "HSI used WHOIS data regularly prior to the implementation of GDPR in May 2018. Subsequent to GDPR, the inability to conduct instant electronic queries has added an extra step and slowed down the investigative process. HSI continues to request and use domain name registrant information via legal process from registrars who maintain that information. The registries and registrars review requests for information and determine if the requestor has the authority, if the order was issued by a court of competent jurisdiction, and whether the request violates any portion of

[4] https://secureandtransparent.org/wp-content/uploads/2021/10/Lawful-and-Legitimate-WHOIS-and-Proxy-Requests-Under-GDPR-DNS-Reveal-Requests-CSTI.pdf

> the GDPR. Unfortunately, there is no centralized point of contact from whom to request the information, and with over 2,000 registrars, some outside of the United States, it is sometimes difficult to determine who to contact **and how to procure a legal order they will recognize and respond to**."

The negative impact of ICANN's misguided implementation of the EU GDPR was demonstrated through a 2021 users' survey conducted by the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG). That survey targeted cyber investigators and anti-abuse service providers to, "determine the impact of ICANN's implementation of the EU GDPR." The survey found that, "**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 our respondents report that redaction [of WHOIS data] impairs their ability to investigate relationships between malicious domains and actors and two-thirds of our respondents indicate that their ability to detect malicious domains has decreased.[5]

Finally, it is worth noting that this domain name registration/WHOIS information had been publicly available prior to the implementation of the EU GDPR. Law enforcement and others could readily access it at their own will and discretion, without any delay, and it was often the first step of any cyber investigation.

Keep in mind that the EU GDPR imposes no requirement to protect the registration data of legal persons, only natural ones. The restrictions placed on the WHOIS data of legal persons is not based on GDPR requirements and arguably is contrary to the goal of the GDPR because the redaction of all of this data has made it more difficult to fight online phishing and other attacks that violate the privacy rights of Internet end users.

Concern: ICANN's leadership's salaries are dependent on domain name registrations

ICANN receives its funding through fees paid by registries and registrars. ICANN's revenues are directly tied to the volume of domain registrations that occur. For example, in its financial year 2020 report, ICANN itself stated: "The domain name market was resilient in the second half of fiscal year 2020 (FY20), despite the pandemic. As a result, ICANN's funding is USD 0.6 million (0.4%) higher than the budget."[6] As succinctly stated by Marketplace.org "ICANN gets paid for every domain name that's registered."[7] It is this funding relationship between the registries and registrar (the regulated) and ICANN (the regulator) that was being highlighted.

---

[5] https://www.icann.org/en/system/files/correspondence/cadagin-shiver-to-marby-et-al-08jun21-en.pdf
[6] https://www.icann.org/en/announcements/details/icann-publishes-fy20-financial-results-15-10-2020-en
[7] https://www.marketplace.org/2014/10/02/how-money-gets-made-when-people-snap-web-domains/

Concern: ICANN ignores complaints from government agencies, particularly about malicious activity related to COVID

Concerns surrounding the implementation of the EU GDPR have existed and been expressed since it went into effect in May of 2018. ICANN also acknowledged the issue and initiated an Expedited Policy Development Process (EPDP) to develop a solution. In April of 2019, then-Administrator of the U.S. National Telecommunications & Information Administration (NTIA) David Redl wrote to ICANN Board of Directors Chair Cherine Chalaby on the status of a resolution for lack of access to WHOIS information. In his letter, Redl states,

> "Yet to be addressed is the development of a technical solution, and policies associated with disclosure and access to non-public WHOIS information. Now it is time to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions. NTIA is expecting the second phase of the EPDP discussion to kick off in earnest in the coming weeks, and to achieve substantial progress, if not completion, in advance of ICANN's meeting in Montreal in November [of 2019]. Without clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered."

Unfortunately, that EPDP effort concluded without a workable solution. That is not solely the opinion of CSTI but rather the final policy recommendation by the Government Advisory Committee (GAC) – which includes U.S. government participation, including from NTIA and the FTC – which stated:

> "[T]he GAC must withhold support for certain Recommendations which in their current form do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars and protecting the public from harms associated with bad actors seeking to exploit the domain name system. In this regard, the GAC highlights that the domain name system is a global public resource that must serve the needs of all its users, including consumers, businesses, registrants, and governments."

Congress, too, has weighed in on this issue. Report language was included in the *Consolidated Appropriations Act for 2021* (P.L. 116-260) which stated:

> "NTIA is directed, through its position within the Governmental Advisory Committee, to work with ICANN to expediate 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."

Furthermore, the FTC has been trying to work with ICANN on potential solutions as it described in its letter to Rep. Latta. The FTC stated:

> The FTC would benefit from greater and swifter access to domain name registration data. Achieving this goal is difficult, however, given the complexity of the GDPR's effect, the required international coordination, and the many stakeholders involved. We have been working with other U.S. agencies to develop solutions through our interaction with ICANN and our international law enforcement colleagues.
>
> One approach that could help overcome the current obstacles would be to mandate disclosure of domain name registration data associated with legal entities, as opposed to natural persons. Legal entities register a significant percentage of domain names, and the GDPR protects the information of natural persons but does not apply to information related to legal entities. ICANN's current mechanisms result in over-application of the GDPR by permitting registrars to choose whether to make the registration data of legal entities public or not. We have raised this issue within ICANN's policy development process."

Despite the lack of WHOIS access being an acknowledged problem since 2018, we remain no closer to a workable solution today than we were either when then Administrator Redl wrote to the ICANN Board or when Congress included its above quoted Report language in the 2021 Consolidated Appropriations Act. Even more discouraging, no functional solution even appears to be on the horizon with respect to ICANN and its policies. CSTI encourages the FDA to engage directly with the National Telecommunication & Information Administration, as the lead entity engaged with ICANN, to express the agency's interest in this issue and request an update on the status of WHOIS policy and the likelihood of seeing access restored.

As the FDA stated in its own letter in response to Rep. Latta dated August 13, 2020:

> "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."

CSTI wholly agrees with this position and applauds the efforts of on-the-ground investigators and law enforcement professionals, like Dan Burke, who are raising their serious concerns over these issues and attempting to foster attention for a much-needed solution.

Thank you for your consideration,

Coalition for a Secure & Transparent Internet

CC: Congresswoman Jan Schakowsky (D-IL)
Congressman Robert Latta (R-OH)