14 June 2022

Robert M. Califf M.D., MACC
Commissioner,
U.S. Food and Drug Administration
10903 New Hampshire Ave
Silver Spring, MD 20993-0002

Dear Dr. Califf:

On June 2, 2022, Mr. Dan Burke, who serves as the U.S. FDA's Chief of the Investigative Services Division, Office of Criminal Investigations, Office of Regulatory Affairs[1], gave a 30-minute presentation during a webinar entitled, "The Threat of a Dark WHOIS: Putting Americans' Health, Safety and Cybersecurity at Risk." Mr. Burke's presentation included certain statements about ICANN, the organization that coordinates the Domain Name System (DNS), as well as the availability of non-public domain name registration information that ICANN helps to coordinate. Without further context, these statements could be misleading. The purposes of this letter are two-fold. First, we wish to offer additional context and corrections to some of Mr. Burke's statements. Second, we urge the FDA to coordinate with the U.S. Government's DNS interagency working group to become informed about ICANN's policies and to raise government-level concerns.

The webinar was sponsored by an entity called the "Coalition for a Secure and Transparent Internet", which according to its website was formed, "to educate federal and international policymakers and stakeholders on the critical importance of open access to WHOIS data, and to advocate for appropriate policy decisions to protect this crucial tool."[2] The following provides additional information to address concerns about ICANN and access to non-public registration data raised by Mr. Burke during his presentation.

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

The presentation suggested that the FDA could not identify the registered name holders for certain domain names because it lacks subpoena power and instead must request the U.S. Department of Justice to obtain subpoenas.

Response: It is not necessary to obtain a subpoena to gain access to non-public domain name registration data. Law enforcement and consumer protection agencies around the globe have relied on existing ICANN WHOIS policies to gain access to this data.

When an Internet user wishes to register a generic top-level domain (gTLD) domain name, that registrant must provide certain personal contact information, including name, address, email, phone number, and technical contact. Under their agreements with ICANN, gTLD registry

---

[1] https://www.fda.gov/about-fda/i-am-ora/i-am-ora-profile-dan-burke.
[2] https://secureandtransparent.org/

operators and accredited registrars must maintain current and accurate gTLD registration data for all of their domain name registrants. This information is referred to as WHOIS data. WHOIS data is not maintained in a single, centrally operated database. Instead, the data is managed by independent entities, located around the globe, that register domain names ("registrars") and run the infrastructure to support them ("registries"). All gTLD registries and registrars have agreements with ICANN that establish requirements related to the handling and disclosure of gTLD registration data.

Prior to the adoption of the European General Data Protection Regulation (GDPR), registrars were required to publish this WHOIS data, including registrants' personal contact information. The GDPR, and the risk of liability arising from GDPR violations, has had a significant impact on the availability of public WHOIS data. Compliance with GDPR has required modifications to the WHOIS system. Under the current ICANN policy, registrars and registries are required to provide public access to non-personal gTLD domain registration data. They must also continue to collect all contact information for domain name registrations but must restrict publication of personal data for registrations with a nexus to the European Economic Area (EEA) (e.g., where the registrant is an EU resident), absent registrant consent. For registrations without an EEA nexus, registries and registrars may choose not to publish personal data on a global basis.

The current policy requires registries and registrars to accept and consider third-party requests for access to full registration data:

> "Registrars and registry operators must provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR."[3]

There is no requirement for requestors to obtain a subpoena or lawful order as a condition of gaining access to a registrant's personal contact information.

In a few instances, government agencies have submitted complaints to ICANN Contractual Compliance regarding registrars' refusal to provide non-public registration data. These agencies were ultimately successful in gaining access to the requested data without having to obtain a subpoena or lawful order. Information on how to submit a complaint regarding access to registration data is available on ICANN's website.[4]

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

Response: ICANN's leadership's salaries are in no way tied to or dependent upon domain name registrations. ICANN remuneration practices, including for the officers of the organization, are transparent and publicly posted.[5]

---

[3] Temporary Specification for gTLD Registration DataAppendix A, Section 4.1 available at
https://www.icann.org/resources/pages/gtld-registration-data-specs-en#appendixA
[4] https://icannportal.force.com/compliance/s/registration-data
[5] https://www.icann.org/en/system/files/files/remuneration-practices-fy22-01jul21-en.pdf.

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

Response: By way of background, ICANN is a California-based nonprofit, public-benefit organization accountable to a global community of stakeholders. ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems, and to coordinate the allocation and assignment of names in the root zone of the DNS through the Internet Assigned Numbers Authority (IANA) functions. (ICANN is the IANA functions operator and controls its performance.) In its role as the technical coordinator of unique identifiers for the Internet, ICANN is not political and, therefore, takes actions to
ensure that the workings of the Internet are not politicized.

ICANN works closely with other technical partners in the Internet ecosystem to help enforce and evolve the rules, initially developed some 40 years ago, to ensure we have one secure, stable, interoperable Internet. ICANN is part of an Internet ecosystem that works together for the global public interest.

As part of its mission to maintain the security and stability of the Internet's unique identifier system, ICANN conducts technical studies on the prevalence of DNS security threats. The Domain Name Security Threat Information Collection & Reporting (DNSTICR) project is an ongoing effort conducted by the ICANN Office of the Chief Technology Officer (OCTO) to look at registrations related to the COVID-19 pandemic to find evidence of any activity related to malware or phishing. Where sufficient evidence of malicious activity is found, ICANN sends a report to the responsible registry or registrar so that they can determine the appropriate action, such as suspending or deleting the domain name.[6]

ICANN grew out of a 1998 commitment from the U.S. Government to transfer coordination of the DNS to a new non-profit corporation based in the U.S. with global participation. For nearly two decades, ICANN performed the Internet Assigned Numbers Authority (IANA) functions under a zero-dollar contract with the U.S. Department of Commerce, implementing policies developed by the multistakeholder community.

The U.S. Government supported the creation of ICANN and the private sector-led approach to Internet governance. Congress and Administrations of both parties have long supported ICANN and its multistakeholder model and have pushed back against efforts by governments and intergovernmental organizations to take over ICANN's role in coordinating the DNS.[7]

---

[6] https://www.icann.org/dnsticr-en.

[7] *See, e.g.,* A Declaration for the Future of the Internet, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (signed on April 28, 2022 by the governments of the United States and 60 other nations, expressing support for ICANN and the multistakeholder system of Internet governance); Testimony of Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, United States House of Representatives, July 8 2005, https://www.ntia.doc.gov/speechtestimony/2015/testimony-strickling-internet-governance-progress-after-icann-53 ("This multistakeholder approach to Internet governance – in which technical experts, civil society, private industry, and governments make policy decisions on a consensus basis – is the best

The U.S. Government actively participates in ICANN through its representation on the Governmental Advisory Committee (GAC). The National Telecommunications and Information Administration within the Department of Commerce is the USG representative to the GAC. The GAC constitutes the voice of Governments and Intergovernmental Organizations (IGOs) in ICANN's multistakeholder structure. Created under the ICANN Bylaws, the GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements.[8]

One of NTIA's long-standing priorities has been to ensure that law enforcement, consumer protection agencies, cybersecurity researchers, and intellectual property owners have efficient and effective access to WHOIS data.[9] NTIA will represent the U.S. Government at the upcoming ICANN74 Policy Forum at which there will be several discussions regarding the issue of access to non-public registration data. The GAC will hold its own session entitled, "WHOIS and Data Protection":

> "This session aims to discuss status and consider possible next steps for the GAC in relation to deliberations and implementation efforts aiming to establish a new WHOIS/Registration Data policy regime taking into account relevant Data Protection law. The GAC will be briefed on latest developments and related policy concerns, possibly in connection with EPDP Phase 1 Implementation, the System for Standardized Access and Disclosure (SSAD) proposed as part of EPDP Phase 2, EPDP Phase 2A Policy Recommendations regarding Legal vs. Natural Persons, and scoping of possible future policy work regarding accuracy of registration data."[10]

NTIA also will participate in the drafting of the GAC Communiqué, which is submitted to the ICANN Board and community following every ICANN Public Meeting. Among other things, the Communiqués convey issues of importance to the GAC and provide advice to the ICANN Board. To date, the GAC has provided several items of advice to the ICANN Board and submitted extensive input regarding access to Whois.[11]

---

mechanism for maintaining an open, resilient, and secure Internet. NTIA greatly appreciates the long-standing bipartisan support for the multistakeholder approach expressed by Congress," citing H.Con.Res. 127 and S.Con.Res. 50 (2012), stating "the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today;" S. Res. 71 (2015), stating "the United States remains committed to the multistakeholder model of Internet governance" and that "the [IANA] transition process demonstrates that the United States supports and is committed to the multistakeholder model of Internet governance.").

[8] https://gac.icann.org/.
[9] *See e.g.,* Remarks of David J. Redl at the State of the Net 2018, Jan. 29, 2018 ("Right now, NTIA has two main priorities internationally. The first is the preservation of the WHOIS service, which has become one of NTIA's most pressing issues related to ICANN over the last several months.") https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-state-net-2018.
[10] https://74.schedule.icann.org/agenda#/?limit=20&skip=10&sortByFields[0]=startsAt&sortByOrders[0]=1&uid=6T5TswJDXJ9Z3dMqN.
[11] https://gac.icann.org/topics/epdpOnGtldRegistrationData (listing several items of advice, correspondence and Communiqués submitted to date on the subject of gTLD Registration data following enactment of the GDPR).

Given the FDA's interest in domain name policies, we encourage your agency to actively participate in the U.S. Government's DNS interagency working group. We would also be happy to provide additional information and answer any questions regarding ICANN and its technical mission.

Sincerely,

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

cc: The Honorable Alan Davidson
Assistant Secretary of Commerce
Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D. C. 20230