August, 13, 2020

The Honorable Robert E. Latta
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Latta:

Thank you for your letter of June 24, 2020 regarding the Coronavirus outbreak (COVID-19) and inspections. We appreciate your interest in ensuring that the Food and Drug Administration (FDA or the Agency) has the necessary tools to combat fraud and ensure the safety and supply of pharmaceuticals, human and animal food, and medical supplies. As you are aware, the U.S. Government is accelerating response efforts due to COVID-19. FDA appreciates your support, and that of Congress, as we all work together toward a united goal of controlling this outbreak.

To that end, we offer the following responses to your specific questions, broken into Criminal and Civil responses, as we have two offices that utilize WHOIS:

1. If and how your office uses or has used WHOIS in the execution of its functions?

Criminal Case Investigations

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.

WHOIS data has also been widely used in FDA's criminal investigations to identify individuals and organizations selling online a variety of unapproved/uncleared/unauthorized products such as opioids, counterfeit or adulterated drugs as well as purported dietary supplements containing deleterious or undeclared ingredients. Most recently, lack of WHOIS transparency significantly hindered FDA's ability to identify sellers of fraudulent and unproven treatments for COVID-19 as well as illegitimate test kits and counterfeit or substandard personal protective equipment. These cases range from a simple website marketplace to sophisticated transnational cybercrime networks involving thousands of websites, hidden servers, dark web applications and virtually linked co-conspirators. Many of these criminal conspiracies were linked or identified via historical WHOIS analysis.

FDA's ability to effectively regulate industry relies on transparency with the manufacturers and distributors of the products regulated by FDA. WHOIS data are frequently used to determine the owner or operator of particular website in the context of our regulatory duties. FDA has used WHOIS data to trace foodborne contamination or product tampering supply chains, contact website owners about illegal or deceptive

U.S. Food & Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
www.fda.gov

marketing or labeling online, as well as to notify online sellers about a company that has recalled products and issue Warning Letters to online sellers.

Finally, WHOIS data are an essential resource in conducting cybersecurity incident response and threat related assessments/investigations. The security and protection of FDA critical assets and infrastructure is often contingent on the identification and validation of the owners and operators of these internet resources. Specifically, the potential loss of access to WHOIS data in the cybersecurity context as part of the enforcement of GDPR would negatively impact FDA's ability to effectively analyze and validate external connections (IP addresses) within the European Union (EU).

Consistent with ICANN's (Internet Corporation for Assigned Names and Numbers) Bylaws, FDA's access to WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."[1] FDA's legitimate interests are also consistent with the recitals to the GDPR, which permit processing of personal data for "preventing fraud;" "ensuring network and information security," and reporting possible "criminal acts or threats to public security" to authorities.[2]

Civil Case Investigations

FDA's Health Fraud Branch (FDA-HFB) routinely accesses WHOIS databases to obtain information on the domain registrants for websites selling FDA-regulated commodities. FDA-HFB has a subscription to a database that also provides historical WHOIS data, as well as other data necessary to conduct internet investigations. FDA-HFB uses and has used WHOIS data to identify the recipients of warning letters, determine responsibility of FDA-regulated operations from a given domain or website, establish connections or relationships among different domains or to gather additional data points (email addresses, phone numbers, IP addresses) as part of Agency investigations.

2. If and how your office has experienced increased difficulty (including delays) in accessing WHOIS information since the May 2018 implementation of the EU GDPR?

Criminal Case Investigations

Although a small number of domestic registrars will offer WHOIS data pursuant to a written request, FDA cannot access WHOIS information without a Grand Jury subpoena, and WHOIS data is no longer available for foreign registrars. Unlike some other federal law enforcement agencies, 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. Because FDA cannot access basic WHOIS data

[1] ICANN Bylaws, Registration Directory Services Review, §4.6(e).

[2] *See GDPR* Recitals 47, 49 and 50.

without a Grand Jury subpoena, which requires coordination with the Department of Justice, many investigative leads have not been sufficiently addressed or significantly hindered.

Civil Case Investigations

More often, the data in WHOIS reports in the searches that FDA-HFB is conducting are either missing, redacted or hidden via a proxy registrant for domains. This proxy service is the point of contact for any inquiries regarding the domain. There are hundreds of ICANN accredited registrars that provide proxy registrant services and in very few instances have these registrants been cooperative in providing non-public data to FDA about the owners and operators of a domain. In some cases, these proxy services refer any inquiries to the domain registrar, which provides only the publicly-available, redacted or missing WHOIS data. FDA-HFB has found that Regulation (EU) 2016/79, or GDPR, extends to domains that may not be operating strictly within the EU. In a recent example, one registrar cited the GDPR compliance requirements as the basis to broadly restrict WHOIS data, claiming the burdensome technical difficulties necessary to differentiate among customers on the basis of their likely geographic locale.

3. If and how your office would be able to more effectively conduct investigations and/or intercede in illegal activity with greater WHOIS access?

Criminal Case Investigations:

Greater WHOIS access would significantly assist FDA with the identification of individuals and firms illegally selling FDA-regulated products online. WHOIS adds a layer of transparency to websites, online marketplaces and vendors, and enables our regulatory, cybersecurity and law enforcement personnel to link seemingly disparate websites into organized affiliated networks and track historical domain name ownership.

In the past, suspects operating ecommerce websites illegally selling FDA-regulated products had to provide point of contact (POC) information. After developing sufficient probable cause, OCI agents investigating fraudsters could use this information as part of an affidavit to obtain search warrants. These search warrants often provided agents with additional investigative leads that helped identify the suspect(s), detailed information on the criminal scheme, location of ill-gotten assets and other items of value in a criminal investigation. Agents could also conduct “reverse WHOIS” searches using POC information provided by the suspects. This data has been used to link the suspect(s) to other affiliated websites. Now that WHOIS information is no longer available, it is extremely time-consuming, and in some instances not possible, for agents to fully identify the entire scope of an illicit online network.

Civil Case Investigations:

FDA-HFB would be able to quickly and efficiently identify and respond to the unlawful sales of FDA-regulated products if complete and accurate WHOIS data were available.

As noted above, establishing connections or determining responsibility of website owners and operators where WHOIS data are redacted or missing can be resource intensive, causing delays that can complicate investigations and cases.

Thank you again for your concern and contacting us regarding this matter. If you have any questions, please let us know.

Sincerely,

Karas Gross

Karas Gross
Associate Commissioner for
Legislative Affairs