Strafford

Presenting a live 90-minute webinar with interactive Q&A

Domain Name Disputes Post-GDPR: Navigating URS, UDRP, ACPA With Reduced Access to Information

WEDNESDAY, NOVEMBER 11, 2020

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Rick Lane, Founder and CEO, **Iggy Ventures, LLP**, Washington, D.C.

Paul D. McGrady, Jr. (Moderator), Partner, **Taft Stettinius & Hollister**, Chicago

Jonathan Uffelman, Domain Name Specialist/Attorney, **Finnegan Henderson Farabow Garrett & Dunner**, Washington, D.C.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

September 2, 2020

Mr. Adam Candeub
Acting Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4275
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association to NTIA on the Need for Reliable Access to the WHOIS Database

Dear Acting Assistant Secretary Candeub,

ACT | The App Association would like to take this opportunity to add our voice to the chorus of stakeholders who realize that a critical juncture in internet governance has been reached with respect to the WHOIS database. The App Association represents more than 5,000 small and medium-sized mobile software and connected device companies around the globe. App Association member companies lead the $1.7 trillion app economy in the United States and employ 5.9 million Americans. The small business community that the App Association represents relies on intellectual property (IP) to grow and create jobs, and the infringement and theft of IP (copyrights, trademarks, patents, and trade secrets) presents a major threat to our members and the billions of consumers who rely on their digital products and services. As such, App Association members strongly benefit from reliable and accurate WHOIS data, which allows them to investigate and contact third parties suspected of IP infringement at the domain level.

As you know, the WHOIS database serves a vital public service to IP holders and the general public alike, acting as essentially the phonebook of internet by publicizing domain name registration data. WHOIS data helps protect internet users from fraud, provides transparency to researchers and academics, and enables cybersecurity professionals to protect against network risks. However, through an overly broad interpretation of Europe's General Data Protection Regulation (GDPR), there has been a strong curtailing of access to WHOIS data recent years. Though the Internet Corporation for Assigned Names and Numbers (ICANN) has authority to restore WHOIS access through its policy development process, it has failed to do so to date. ICANN's latest output on the topic, the Final Report of Phase 2 of the Expedited Policy Development Process (EPDP) on generic top-level domain (gTLD) Registration Data, for example, does not substantively address any of the current concerns about the accessibility, accuracy, or reliability of WHOIS data.

The App Association finds this current lack of access to domain name registration data through the WHOIS database unacceptable and threatening to both intellectual property owners, such as our member companies, and to the security and stability of the internet

itself. The App Association, therefore, respectfully requests the Administration take a proactive posture toward this important issue and determine how it can restore WHOIS to the state that internet users came to know and expect prior to May 2018.

We appreciate and thank you for your time and attention to this important issue. The App Association looks forward to working with you to create a better internet for all.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Privacy Fellowship Coordinator

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

Office of Congressional Relations

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

July 16, 2020

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

Dear Representative Latta:

Thank you for your June 24, 2020 letter to U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI) and the National Intellectual Property Rights Coordination Center (IPR Center) regarding the European Union's General Data Protection Regulation (GDPR) and its impact on HSI's ability to obtain WHOIS information in support of its criminal investigations.

HSI uses domain name registration information, previously available via online WHOIS query, to aid in the identification of persons or entities responsible for registering domains that are used to conduct a wide variety of crimes, which include intellectual property crimes, cyber-crimes (such as theft of personally identifiable information [PII] and credit card information), crimes related to illegal importation and exportation of goods, and the promotion and distribution of child sex abuse material.

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 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. In addition to slowing the process to get registrant information, the likelihood of getting a judicial order for the release of information can be difficult since a number of requests are made in the initial stage of an investigation or response and agents may not have enough information on the criminal activity to satisfy necessary requirements. Lastly, due to the penalties that can be imposed by GDPR for improper release of a registrant's PII, many registries and registrars are redacting registrant information regardless of whether or not the subject is a citizen within the European Union.

As a recent example of GDPR inhibiting HSI investigations, the HSI Cyber Crime Center (C3) Cyber Crimes Unit identified several websites posing as legitimate coronavirus disease 2019 (COVID-19) fundraising organizations, but are actually fraudulent. These websites claim to be sites for entities such as the World Health Organization, United Nations' foundations, and other non-governmental organizations, and appear to be legitimate. When HSI conducted WHOIS queries for these domains, most of the subscriber information was redacted as a result of GDPR. Having

increased and expedient access to domain name registration information would have allowed HSI to identify the registered owners of the domains expeditiously in order to prevent further victimization by these illegitimate fundraising websites. When HSI is required to use legal process (e.g. administrative subpoenas, non-disclosure orders, or grand jury subpoenas) to obtain registrant information, this can cause delays and potentially negatively impact an investigation.

HSI views WHOIS information, and the accessibility to it, as critical information required to advance HSI criminal investigations, including COVID-19 fraud. Since the implementation of GDPR, HSI has recognized the lack of availability to complete WHOIS data as a significant issue that will continue to grow. If HSI had increased and timely access to registrant data, the agency would have a quicker response to criminal activity incidents and have better success in the investigative process before criminals move their activity to a different domain.

In an effort to address the challenge of limited WHOIS information as a result of GDPR, the HSI C3 has assigned full-time representatives to the Public Safety Working Group (PSWG) within the Internet Corporation for Assigned Names and Numbers (ICANN) organization. The PSWG is comprised of law enforcement and consumer protection agencies that work closely with various constituencies that are represented within the ICANN ecosystem. In the absence of a more viable solution, HSI C3 members on the PSWG continue to work with registries, domain registrars, and civil society groups to develop a consensus solution for access to domain name registration information within the ICANN framework and compliant with GDPR.

Thank you again for your letter and interest in this matter. Should you wish to discuss this matter further, please do not hesitate to contact me at (202) 732-4200.

Sincerely,

Sean Hackbarth
for

Raymond Kovacic
Assistant Director
Office of Congressional Relations

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Chairman

July 30, 2020

The Honorable Robert E. Latta
United States House of Representatives
Washington, D.C. 20515

Dear Representative Latta:

Thank you for your June 24, 2020 letter requesting information about how the Federal Trade Commission ("FTC" or "Commission") uses domain name registration information, also known as WHOIS, to carry out its law enforcement mission, including its efforts to stop frauds related to COVID-19. You also highlighted your concerns that the implementation of the European Union's General Data Protection Regulation ("GDPR") has negatively affected the ability of law enforcement to identify bad actors online. I share your concerns about the impact of COVID-19 related fraud on consumers, as well as the availability of accurate domain name registration information.

Since the beginning of the pandemic, the FTC has been monitoring the marketplace for unsubstantiated health claims, robocalls, privacy and data security concerns, sham charities, online shopping fraud, phishing scams, work at home scams, credit scams, and fake mortgage and student loan relief schemes, and other deceptions related to the economic fallout from the COVID-19 pandemic.[1] In response, we have taken actions, including filing four cases in federal courts and sending hundreds of warning letters to businesses in the United States and abroad.[2] In addition, we have conducted significant public outreach and education efforts.[3]

Before the GDPR took effect in May 2018, the FTC and other consumer protection and law enforcement agencies routinely relied on the publicly-available registration information about domain names in WHOIS databases to investigate wrongdoing and combat fraud.[4] The FTC uses this information to help identify wrongdoers and their locations, halt their conduct, and preserve money to return to defrauded victims. Our agencies may no longer rely on this information because, in response to the GDPR, ICANN developed new policies that significantly limit the publicly available contact information relating to domain name registrants. For

---

[1] *See generally* Prepared Statement by the Federal Trade Commission before the S. Comm. on Commerce, Science, and Transp., Subcommittee on Manufacturing, Trade, and Consumer Protection: Consumer Protection Issues Arising from the Coronavirus Pandemic (July 21, 2020), https://www.ftc.gov/public-statements/2020/07/prepared-statement-federal-trade-commission-consumer-protection-issues.

[2] *See generally* https://www.ftc.gov/coronavirus. This page is updated regularly.

[3] *Id.*

[4] *See, e.g.*, Comment of the Staff of the FTC Bureau of Consumer Protection before the ICANN Public Comment Forum, In the Matter of Tentative Agreements among ICANN, U.S. Dep't of Commerce, and Network Solutions, Inc. (Oct. 29, 1999), https://www.ftc.gov/policy/policy-actions/advocacy-filings/1999/10/ftc-staff-comment-internet-corporation-assigned-names; Prepared Statement of the Federal Trade Commission, Hearing on Internet Governance: The Future of ICANN, Before the Subcommittee on Trade, Tourism, and Econ. Dev. of the S. Committee on Commerce, Science, and Transp., 109th Cong. (Sept 20, 2006), http://www.ftc.gov/os/testimony/P035302igovernancefutureicanncommissiontestsenate09202006.pdf.

example, 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. This can be a time-consuming and cumbersome process.[5]

This lack of access also limits consumers' ability to identify bad actors using WHOIS information. Prior to the GDPR, thousands of the complaints filed in our Consumer Sentinel complaint database referred to the filer's use of WHOIS data to identify businesses involved in spyware, malware, imposter scams, tech support scams, counterfeit checks, and other malicious conduct.[6]

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.

I appreciate your interest in these issues. If you or your staff has additional questions or comments, please contact Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195.

Sincerely,

Joseph J. Simons

Joseph J. Simons
Chairman

[5] There are more than 2,500 ICANN accredited registrars, many located outside the U.S., with different procedures to obtain registrant data. It can be challenging to determine where to direct a request and what to include in such request for access to this now non-public information as many registrars fail to place such guidance in a location that is easy to find on their websites. After submitting a request, the FTC must wait for the registrar to approve or reject our requests. Moreover, when data is located in a foreign jurisdiction, the process may be more time consuming and require cooperation from our law enforcement partners.

[6] In 2017, we identified over 4,000 complaints filed over a five-year-period.

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