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.