



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