February 28, 2020

Chairman Roger Wicker
Senate Committee on Commerce, Science, & Transportation
512 Dirksen Senate Building
Washington, DC 20510

Ranking Member Maria Cantwell
Senate Committee on Commerce, Science, & Transportation
425 Hart Senate Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell,

We the undersigned organizations write in support of the vital role that WHOIS domain name registration data plays in protecting consumers and businesses from criminal networks and its role in cyber security and cyber investigations. While the value of WHOIS data is widely known throughout the cyber security industry, its day-to-day use is less known elsewhere. We are gravely concerned about the overly broad interpretation and damaging implementation of the European Union's General Data Protection Regulation that has effectively blocked access to this critical data set and the time has come for Congress to engage on this important issue.

As you may know, WHOIS data is the publicly available information on *who* has registered a particular internet domain name. In layman's terms, WHOIS records are akin to land title or property tax records: a record of who owns the internet property of domain names available in .com, .net, and other generic top-level domain (gTLD) spaces. Each WHOIS record contains basic contact information for the domain name registrant: name, address, phone number and email address, and certain other technical attributes. Since the dawn of the internet as we know it, gTLD registrars and registries – those companies who sell domain names – have collected contact information from all registrants at the time of registration.

WHOIS data is critical to law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, intellectual property rightsholders, journalists, academics and others. These stakeholders all rely on WHOIS to help them determine *who is* operating a criminal website, sending malicious (spam, phishing) emails, conducting cyber-attacks, propagating fake news or committing fraud under the guise of a known brand. In these instances, WHOIS data is used to identify and collect lists of domain names that investigators associate with a given criminal or cyber-attack and to identify the likely perpetrators of these attacks. In criminal investigations, for example, listing domains and making connections using contact information is imperative to understanding and interdicting criminal, terrorist, or hostile nation state activity to its fullest extent.

Because of an overly broad interpretation of the EU's General Data Protection Regulation (GDPR), many domain name registrars and registries are shutting down public access to WHOIS data. This has the effect of impeding our cyber investigations, limiting our ability to protect American consumers and businesses, and destabilizing the security of the open web. Already, cyber investigators and counter-terrorist agents are experiencing difficulties in utilizing the WHOIS database to the degree it was available prior to the interpretation of the EU GDPR and we expect this issue to continue to worsen.

While efforts have been undertaken by the Internet Corporation for Assigned Names and Numbers (ICANN) to develop an access model moving forward, those efforts have to date proven unsuccessful and the more time lapses without resolution, the less safe U.S. citizens, businesses and institutions will be. Jason Gull, Senior Counsel in the Department of Justice's Computer Crime and Intellectual Property Section spoke at an October 2019 Capitol Hill briefing on WHOIS and commented, "We are finding that WHOIS is turning into 'WHOWAS.' We have historical information about WHOIS from a year ago and the information is like having an old phonebook."[i] Every day, that historical information becomes less relevant.

The National Telecommunications and Information Administration (NTIA) noted in an April 2019 letter that WHOIS, "is a critical tool" for law enforcement cyber security researchers and in intellectual property protection and stressed the importance of the creation of a timely solution that ensure access to WHOIS for law enforcement and third-party interests. That letter expected "significant progress" by the November 2019 ICANN meetings in Montreal[ii]. Those meetings have now come and gone without any notable steps toward a resolution.

The impact of this most recent missed deadline pushes the hope of an acceptable resolution another 12 - 18 months – at minimum - as policies must be agreed to and any eventual access model will take time to be implemented. Meanwhile, criminals and their international networks can operate unencumbered pulling in record profits from their cybercrimes. With the continued proliferation of criminal actors online, law enforcement, government agencies, security experts and researchers are already under strain to keep up with these increasingly sophisticated cybercrimes. These records also are indispensable for tracking down victims, sources and the cybercriminals themselves.

We call upon Congress to act on this critical issue.

Sincerely,

American Apparel & Footwear Association (AAFA)
ACT: The App Association
Alliance for Safe Online Pharmacies (ASOP Global)
Association of American Publishers (AAP)
Americans for Securing All Packages (ASAP)
American Intellectual Property Law Association (AIPLA)
American Pharmacists Association

Association of Home Appliance Manufacturers
Center on Illicit Networks and Transnational Organized Crime (CINTOC)
Coalition for Online Accountability
Coalition for a Secure & Transparent Internet (CSTI)
Domain Tools
Fashion Jewelry & Accessories Trade Association
G2 Verisk
Getty Images
Gilead
Halloween Industry Association, Inc. (HIA)
Intellectual Property Owners Association
Juvenile Products Manufacturers Association, Inc. (JPMA)
KnujOn Solutions LLC
Kroll
LegitScript
Liberty Shared
Motion Picture Association (MPA)
National Association of Boards of Pharmacy (NABP)
National Cyber-Forensics and Training Alliance (NCFTA)
Oracle Corporation
Partnership for Safe Medicines
Pharmaceutical Security Institute
Recording Industry Association of America
Shutterstock Inc.
SpamHaus
Sylint (Cyber Security, Forensics, & eDiscovery)
Transnational Alliance to Combat Illicit Trade (TRACIT)
The Copyright Alliance
The Toy Association
The Gerontological Society of America
Tim K. Mackey (Associate Professor, Director of Health care Research & Policy) - UC San Diego, School of Medicine
UL, LLC

---

[i] "DEA and DOJ Speak at CSTI's Capitol Hill Briefing." https://secureandtransparent.org/dea-and-doj-speak-at-cstis-capitol-hill-briefing/. October 2019.
[ii] "Letter from NTIA Administrator David Redl to Cherine Chalaby." https://www.icann.org/resources/correspondence/1221943-2019-04-04-en. April 2019.