
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

December 16, 2022

Re: Impersonation NPRM, R207000

On behalf of the Coalition for a Secure & Transparent Internet (CSTI), we offer the following comments in response to the Federal Trade Commission's (FTC's) rulemaking, "Trade Regulation Rule on Impersonation of Government and Businesses."

CSTI is a coalition of stakeholders aligned over their shared concerns surrounding the loss of access to domain name registration information, also known as "WHOIS." As the Commission knows, WHOIS information tells us *who is* behind a domain name or website and had been publicly available from the dawn of the modern Internet until an overly broad interpretation of the European Union's General Data Protection Regulation (GDPR) was implemented in 2018. Our loss of access to this information has made confirming who is on the other side of the screen increasingly difficult, if not impossible for normal Internet consumers and even law enforcement, cyber security investigators, consumer protection agencies, and brand owners. In the online world, having access to domain registration information is critical to verifying whether an entity is who they say they are, or impersonating someone else. This issue is exacerbated in times of crisis – like we saw during the COVID pandemic.

Additionally, without access to WHOIS information, neither consumers or governmental agencies can initiate effective litigation – such as restraining orders – to protect individuals and organizations against false-flag sites.

CSTI believes that the FTC should extend coverage in its rule to include the creation of false or misleading domain names or other Internet identifiers and to require the collection and enable access to accurate and complete domain name registration information.

The FTC notes in its rulemaking that among its objectives is to expand the remedies available to it in combatting common and injurious forms of fraud. In 2020, Congressman Latta (R-OH) wrote to several federal agencies about the impact the loss of access to WHOIS information has had on combating fraud and protecting consumers. In response to that inquiry, the FTC noted that:

> "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. T**he FTC uses this information to help identify wrongdoers and their**

> **locations, halt their conduct and preserve money to return to defrauded victims**."[i] (emphasis added)

Clearly the connection between fraud and domain name registration information has enormous ramifications for not only identifying that an impersonation is taking place, but also ensuring that remedies can be pursued for the injured party.

The Department of Homeland Security's Homeland Security Investigations (HSI) responded similarly to an identical inquiry from Rep. Latta (R-OH), noting:

> "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."**[ii] (emphasis added)

In its response, HSI raises a critical point to stopping these fraudulent activities (including impersonation), and that is the need to identify all domain name registrations that are used in the perpetration of a criminal activity. Consider the study conducted by Interisle Consulting Group ("*Criminal Abuse of Domain Names: Bulk Registration and Contact Information Access*") which found that "cybercriminals take advantage of bulk registration services to "weaponize" large numbers of domain names for their attacks.[iii] :Domain name registration information, and the databases that contain that information, enable that level of analysis and give us the ability to understand how these networks are connected and deny their access before harm occurs.

The FTC has also been vocal on the role domain name registration plays in combatting fraudulent activity and, specifically, in empowering consumers to protect themselves.
In its response to Rep. Latta, the FTC noted how the loss of access to this information, broadly, has limited the resources consumers could use to verify who is on the other side of the screen:

> "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 compliant 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.**"[iv] (emphasis added)

These complaints served as "force multipliers" for enforcement agencies as they initiated many investigations into fraudulent activity.

The U.S. Food & Drug Administration also weighed in on its use of domain name registration information and its role in combating fraud:

> "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 website, 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**." (emphasis added)

The FTC's inclusion of the creation of false or misleading domain names or other Internet identifiers is supported by both the CAN-SPAM Act (P.L. 108-187) and the Anticybersquatting Consumer Protection Act (P.L. 106-113). The CAN-SPAM Act requires that for any commercial message, "the originating domain name and email address – **must be accurate** (emphasis added) and identify the person or business who initiated the message."[v] This requirement is a vital first step for consumers to verify the identity of the individual with whom they are engaged. The Anticybersquatting Consumer Protection Act prohibits the use of 'identical or confusingly similar' marks or other intellectual property for profit. Recognizing the ease with which someone can impersonate another online, the Anticybersquatting Consumer Protection Act also extended that prohibition to include domain names.[vi]

CSTI appreciates the opportunity to comment on the underlying question and stands ready to work with the FTC in pursuing remedies that can effectively and efficiently help to verify the identities of those attempting to impersonate another entity. At the core of any online scam, be it malware, ransomware, phishing, or cyber-attack, is a registered domain name. For a rule with a stated goal to "prohibit the impersonation of government, business, or their officials," accurate, accessible WHOIS data is critical.

CSTI would also encourage the FTC to work with Congress on legislation to ensure increased and timely access to domain name registrant data that governments and business need to respond to criminal activity incidents, including impersonation and fraud attacks." Given FTC's role on the Governmental Advisory Committee (GAC), which advises the ICANN board, it has an important voice in this ongoing debate.

Sincerely,

The Coalition for a Secure & Transparent Internet (CSTI)

---

[i] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[ii] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[iii] https://www.interisle.net/criminaldomainabuse.html
[iv] https://secureandtransparent.org/federal-agencies-stress-important-of-whois/
[v] CAN-SPAM Act: A Compliance Guide for Business | Federal Trade Commission (ftc.gov)
[vi] https://www.govinfo.gov/content/pkg/PLAW-106publ113/pdf/PLAW-106publ113.pdf