



United States Senate  
Committee on Commerce, Science, and Transportation  
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security  
512 Dirksen Senate Building  
Washington DC, 20510

November 27, 2018

Dear Chairman Moran and Ranking Member Blumenthal:

The Coalition for a Secure and Transparent Internet (CSTI) writes to thank you for your leadership on the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security. In response to the hearing being held today, titled "Oversight of the Federal Trade Commission," we write to encourage the subcommittee and the FTC to do all you can to make WHOIS registration data publicly available in order to help protect Internet users from online criminal activity and to enable action against network and cyber security risks, intellectual property violations, and consumer fraud and abuse online.

As you know, WHOIS data is the publicly available information on who has registered and administers generic top level domain (gTLDs) names in spaces like .com and .net as well as certain country-code domain spaces like .TV. WHOIS data has been publicly accessible for free since the inception of the Domain Name System. Generic top-level domain name registrars and registries are contractually required to collect contact information from all domain name registrants at the time of registration. This contact data, including name, address, phone number, and email address, is combined with certain other attributes of a domain name's registration to comprise WHOIS data.

Due to 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 the full range of WHOIS data, both for one-off requests and automated access. Law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, copyright and trademark holders, journalists, academics, and others rely on WHOIS to help determine *who is* operating a criminal website, sending malicious (SPAM, phishing) emails, or initiating cyber security attacks. When WHOIS data goes dark it takes away a critical source of information that is used to help keep the internet safe, secure and sustainable for all internet users.

Comments by Steven Wilson, Head of the European Center for Cybercrime, at the recent ICANN meeting in Barcelona, underscore this point. He stressed that the GDPR has "created an unintended consequence for law enforcement and WHOIS and is now starting to impact significantly on law enforcement judicially and ultimately public safety."<sup>1</sup> Wilson explained that WHOIS has been instrumental in everything from taking down an ISIS network to solving an investigation of a child abuse network, but both Europol and Interpol are now finding that investigations are being slowed down or hindered because of the lack of WHOIS records.

---

<sup>1</sup> <https://static.ptbl.co/static/attachments/191805/1540247405.pdf?1540247405>

These challenges are not just limited to the EU. Only last month, at a hearing held by the Senate Caucus on the International Narcotics Control, Daniel Burke, Senior Operations Manager, Cybercrime Investigations Unit of the U.S. Food & Drug Administration testified that the lack of access to WHOIS data is impairing the FDA's efforts to combat the illegal online sales of opioids: "Conducting online investigations is not easy, and FDA has a narrow, but important role in combatting the online sale of opioids. For good or bad, much of the Internet ecosystem, including dark nets, have adapted and changed to build in anonymity. Public information about the owner of a domain name, known as "whois" data, is now often impossible to access with the implementation of the GDPR."<sup>2</sup> Many groups have been relying on historic WHOIS data that pre-dated GDPR, but as this data goes stale, more and more organizations and government agencies are being hindered in their investigative efforts.<sup>3</sup> When WHOIS data goes dark it takes away a critical source of information that is used to help keep the internet safe, secure and sustainable for all internet users.

Thank you again for your time and attention to this important issue. CSTI and our member organizations look forward to working with you on future versions of the language as you receive feedback, and on other efforts to ensure robust access to the WHOIS database continues. Please contact CSTI via Libby Baney ([Libby.Baney@faegrebd.com](mailto:Libby.Baney@faegrebd.com)) or Josh Andrews ([Josh.Andrews@Faegrebd.cm](mailto:Josh.Andrews@Faegrebd.cm)) anytime.

Sincerely,  
The Coalition for a Secure and Transparent Internet  
[www.SecureandTransparent.org](http://www.SecureandTransparent.org)

ACT | The App Association; Alliance for Safe Online Pharmacies; Coalition for Online Accountability; Crucial Point LLC; CTO Vision; DomainTools; LegitScript; National Association of Boards of Pharmacy; Recording Industry Association of America; Motion Picture Association of America and SpamHaus

---

<sup>2</sup> <https://www.drugcaucus.senate.gov/sites/default/files/FDA%20Testimony%20on%20Fentanyl%20final.pdf>

<sup>3</sup> <https://blog.domaintools.com/2018/09/whois-data-more-important-than-ever/>