Coalition for Online Accountability
COA

Before the
National Telecommunications and Information Administration
Washington, D.C. 20230

In the Matter of	)	
Developing the Administration's Approach to Consumer Privacy	)	Docket No. 180821780-8780-01
Notice of Inquiry	)	RIN 0660-XC041

The Coalition for Online Accountability (COA) appreciates this opportunity to respond to the Notice of Inquiry on Developing the Administration's Approach to Consumer Privacy ("NOI") 83 Fed. Reg. No. 187, 48600 (September 26, 2018).

ABOUT COA

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners, all of them deeply engaged in the use of the internet to disseminate creative works. The COA members are Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); NBCUniversal; The Walt Disney Company; Twenty-First Century Fox; and WarnerMedia. The Coalition's main goal since its founding nearly two decades ago (as the Copyright Coalition on Domain Names) has been to preserve and enhance online transparency and accountability. Consequently, a predominant focus of COA has been to ensure that data concerning domain name registrations and IP address allocations remain accessible, accurate and reliable, as key tools in the fight against online infringement of copyright. This data is also essential in combatting trademark infringement, cybersquatting, phishing, malware and other cyberattacks and a wide array of other fraudulent, abusive and illegal activity online.

COMMENTS

The risk-based flexibility approach to advancing consumer privacy interests while protecting prosperity and innovation set forth in the NOI should ensure that vital public interests concerning consumer safety and security and in combatting rampant illegal activity online are also taken into account. Privacy is clearly an important imperative, but it should not serve as a shield for illegal activity. Moreover, privacy is not an absolute right. Some point to the European Union's General Data Protection Regulation ("GDPR") as setting a very high standard for privacy rights. But even the GDPR explicitly recognizes that "the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights."[1] We therefore urge NTIA to recognize that in furthering consumer privacy via a flexible approach, a balance must always be struck between legitimate privacy interest and other interests such as consumer safety, transparency and the need for data to enforce a broad range of other rights. Such other rights range from the rights of children not to be abused by the creation and distribution online of child sexual abuse materials to the intellectual property rights of creators and innovators.

Our concern for this balance has been heightened by the recent actions undertaken by ICANN with respect to WHOIS data and ICANN's efforts to comply with the GDPR. ICANN has adopted a Temporary Specification that requires the redaction of much of this data, which for decades was publicly accessible. We appreciate that NTIA has expressed concerns about ICANN's over-broad approach.[2] Furthermore, we wish to re-emphasize that certain data about operators of websites and domain name registrants, such as name, e-mail address and other contact information, should be readily accessible. Furthermore, the accessibility of such data about domain name registrants and website operators should not be viewed as somehow at odds with strong levels of privacy protection. To the contrary, ensuring transparency and accountability on the part of domain name registrants and website operators serves to help protect the privacy rights of online users from phishing attacks, identity theft and other scams that seek to steal sensitive private information from users and abuse that information for illicit purposes.

Earlier this year, the Department of Commerce and the Department of Homeland Security issued a Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats.[3] This extensive Report cites to the importance of WHOIS data in combatting the threats. In particular, the Report notes "[Registries] and registrars can facilitate attribution of bad actors by maintaining accurate WHOIS databases. In addition, the federal government

---

[1] See Recital (4) of the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

[2] See COA's comments to NTIA NOI re: International Internet Policy Priorities, page 2. https://www.ntia.doc.gov/files/ntia/publications/coa_response_to_ntia_noi_final_july_17_2018_1.pdf

[3] *See*: Report https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

should work to engage with its European counterparts to ensure that timely access to WHOIS information is preserved as the European data privacy protections are enforced to preserve a critical tool for domestic and global efforts to investigate botnets."[4]

WHOIS information is not only critical for investigation of botnets; it is also essential for investigating and combatting a wide range of illegal online activity that threatens public safety as well as the privacy of internet users. Brian Krebs, a leading American cybersecurity expert, has written that "WHOIS is probably the single most useful tool we have right now for tracking down cybercrooks and/or for disrupting their operations. . . . WHOIS records are a key way that researchers reach out to Web site owners when their sites are hacked to host phishing pages or to foist malware on visitors. These records also are indispensable for tracking down cybercrime victims, sources and the cybercrooks themselves."[5]

The NOI notes that the Administration seeks feedback on a number of high-level goals for Federal action. One of those goals is "Employ a risk and outcome-based approach." (Goal #4). We agree with that goal. The NOI goes on to describe the need for "flexibility to balance business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs, when making decisions about how to adopt various privacy practices." We agree that balance is essential, but wish to stress that other critical inputs include public safety, transparency and combatting illegal activity. These elements must be given due weight in assessing the balance. In seeking to achieve the proper balance and the Administration's articulated goals for protecting consumer privacy, we urge—particularly in the context of the online environment—that public safety, accountability, transparency and combatting illegal activity are always factored into the analysis. Furthermore, in the context of WHOIS data, we support the Administration's continued efforts to rectify the dangerous imbalance that ICANN has created with respect to over-redaction of WHOIS data.

CONCLUSION

Thank you for the opportunity to submit these comments. We would be happy to answer any questions NTIA may have about this submission and look forward to working with NTIA on these important consumer privacy issues.

Respectfully submitted,

Dean S. Marks
Executive Director and Legal Counsel
Coalition for Online Accountability
ed4coa@gmail.com

[4] Ibid., p. 40
[5] See: https://krebsonsecurity.com/2018/03/who-is-afraid-of-more-spams-and-scams/