

GBOC

Global Brand Owner and Consumer Protection Coalition

July 17, 2018

Attn: Fiona Alexander
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, District of Columbia 20230
iipp2018@ntia.doc.gov

RE: *International Internet Policy Priorities* [Docket No. 180124068-8068-01]

Ms. Alexander:

On behalf of the Global Brand Owner Coalition (GBOC), we are grateful for the opportunity to submit the following comments in response to the National Telecommunications and Information Administration (NTIA) Notice of Inquiry on International Internet Policy Priorities.

GBOC is an organization of global businesses and brand owners working together to address common concerns in the online consumer and brand protection space. Founded in November 2017 to address current challenges facing brand owners and consumers in the Internet ecosystem, current members include major US-based businesses across a variety of industries, including computer software, social media, telecommunications, hospitality, and apparel. In particular, GBOC has focused on preserving access to WHOIS data for legitimate intellectual property and consumer protection purposes, in light of changes to domain name registration data processing practices and requirements precipitated by the European Union General Data Protection Regulation (GDPR). However, GBOC has also advocated the preservation and strengthening of trademark rights protection mechanisms (RPMs) in the Domain Name System (DNS), a general respect for international legal norms in DNS policy development (including in efforts to expand the DNS through launches of new generic Top Level Domains (gTLDs)), and enhanced efforts to combat abusive practices by Internet Service providers (ISPs) including domain name registry operators and registrars. We firmly believe these topics coincide with top International Internet Policy Priorities in Internet governance, and we encourage NTIA to continue to support US stakeholders in connection with these matters.

Privacy and Data Protection.

As GBOC has pointed out in prior public comments, most businesses, brand owners, consumer protection agencies, law enforcement agencies and cybersecurity professionals rely on access

to WHOIS data to perform a variety of key functions in the public interest.¹ This data is vital in enabling such parties to detect and combat cybersecurity threats, phishing and other fraud, and websites selling counterfeit or otherwise illegal goods that could harm consumers. In light of recent changes to international privacy laws, primarily the GDPR, ICANN implemented an interim WHOIS system² that substantially reduces access to key data. Such changes go beyond the requirements of the GDPR, whose protections are intended to apply only to the personal data of natural persons (i.e. not legal entities) within the territory of the European Economic Area. However, ICANN's current WHOIS model applies to all registrant types globally. It also provides no unified framework for obtaining access to non-public data. Instead, individual registry operators and registrars are left to make case-by-case evaluations of requests for non-public data, based on no universal minimum criteria, applying *ad hoc* tests to weigh the legitimate interests of the data requestor against the data subject's right of privacy.

These changes to WHOIS service have significantly disrupted brand protection and other efforts that protect consumers and Internet users generally from harm. The currently fractured and non-transparent environment cuts against the free and open Internet that has allowed e-commerce and free speech to thrive. Accordingly, GBOC encourages the NTIA to continue to prioritize efforts to aid in the development of an immediate and more balanced solution for domain name registration data that is more harmonized in terms of access and limits the redaction of available information only to what is absolutely necessary to comply with applicable privacy law. We also support the development of a US legislative solution that would require open access to domain name registration or website ownership data, either via WHOIS or via publication on a relevant website or other online resource.

Multistakeholder Approach to Internet Governance.

GBOC supports the multistakeholder approach to Internet governance in principal as a means for the Internet to continue to grow and thrive, and as the clear alternative to strictly intergovernmental approaches to governance. However, accountability within this multistakeholder approach remains a primary concern for GBOC, whose members depend upon intervention by intermediary service providers--and their accrediting bodies in particular--to remedy malicious conduct and other illegal activity online, including malware, denial of service attacks, phishing, identity theft, fraud, copyright piracy and the sale of counterfeit goods.

GBOC firmly believes that such accountability must remain a top priority for the NTIA. In particular, as compared to the hierarchy of the DNS, the IP address system currently lacks any meaningful accountability. When Internet service providers such as web hosts go rogue, are

¹ See, e.g., GBOC, COMMENTS ON PUBLISHED ICANN PROPOSED INTERIM MODEL FOR GDPR COMPLIANCE (Mar. 10 2018), available at <https://www.icann.org/en/system/files/files/gdpr-comments-gboc-icann-proposed-compliance-models-10mar18-en.pdf>.

² See ICANN, Temporary Specification for gTLD Registration Data (May 17, 2018), available at <https://www.icann.org/resources/pages/gtld-registration-data-specs-2018-05-17-en#temp-spec>.

complicit in, or otherwise turn a blind eye to criminal activity, there are currently zero available accountability mechanisms short of civil litigation or law enforcement intervention. Regional Internet Registries (RIRs) are not typically concerned with evidence that their IP address resources are used to host vast networks of websites engaged in illegal conduct, shielded by one of their members. And most RIRs will only revoke those IP addresses, or de-accredit their members based on purposefully false or fictitious point of contact information, and then only after affording ample opportunity to provide alternative and equally obstructive point of contact details.

Accountability improvements also need to be made within the hierarchy of the DNS. For example, the ICANN contractual compliance department continues to stay true to its strict constructionist mantra that it will only enforce the letter of its contracts with registries and registrars. The Public Interest Commitment Dispute Resolution Procedure (PICDRP) against Top Level Spectrum (registry operator for the .FEEDBACK TLD) serves as the best example of why this mantra is a problem and where NTIA needs to step in to force change toward compliance with US law by contracted parties and greater accountability by ICANN as an accrediting body. In particular, the panel determination in that dispute explicitly acknowledged that the .FEEDBACK registry agreement “imposes no obligation on ... the registry operator itself to avoid fraudulent and deceptive practices.”³ ICANN declined to take remedial action against the fraud and other illegal acts identified in that case, and subsequent accountability mechanisms have proven unavailing. In sum, the NTIA and other governmental actors should take all action necessary to ensure that registry operators must, as a contractual matter, abide by all applicable laws and governmental regulations.

Finally, meaningful RPMs are an integral first option for intellectual property enforcement online, such that escalation through voluntary industry mechanisms, ICANN accountability mechanisms, law enforcement referrals and litigation, all need not be pursued in every single case. However, these same RPMs, which include the tried-and-tested Uniform Domain Name Dispute Resolution Policy, remain under constant threat from a relatively small cohort of domain name speculators and data privacy maximalists who would see them diluted or abolished entirely. The fact that only a few individuals alone can influence, and in some instances even capture, such policy matters within ICANN stands as both a testament, and perhaps the strongest threat to, the multistakeholder model. The NTIA, through its role on the Governmental Advisory Committee, must continue to serve as an emergency backstop to such threats, particularly with respect to the RPMs.

Conclusion

³ See ICANN, Notice of Breach of Registry Agreement, at p. 17 (March 16, 2017) available at https://www.icann.org/uploads/compliance_notice/attachment/911/serad-to-westerdal-16mar17.pdf (visited July 17, 2018).

We greatly appreciate the opportunity to provide GOC's comments regarding International Internet Policy Priorities. We look forward to continuing to engage with NTIA to educate other parts of the US Government, private stakeholders, and individual consumers about these important issues. Thank you very much for your continued efforts in this regard.

Please contact GBOC at any time if we can be of further assistance, by reaching out to GBOC counsel Brian J. Winterfeldt (brian@winterfeldt.law) and the Winterfeldt IP Group team (internet@winterfeldt.law).