COALITION FOR ONLINE ACCOUNTABILITY

WEBSITE: WWW.ONLINEACCOUNTABILITY.NET E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

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

In the Matter of	)	
International internet Policy Priorities	)	Docket No. 180124068-8068-01
Notice of Inquiry	)	RIN 0660-XC041

The Coalition for Online Accountability (COA) appreciates this opportunity to respond to the Notice of Inquiry on International internet Policy Priorities ("NOI") 83 Fed. Reg. No. 108, 26036 (June 5, 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.

INTRODUCTION

Free flow of data and information and an open and interoperable internet are goals that have been properly embraced by NTIA and the United States government overall, and that all stakeholders should be able to support. Unfortunately, these goals are sometimes misinterpreted to mean that the rule of law should not apply online and that illegal activity conducted online should somehow be given a free pass. While there is no doubt that the borderless nature of the internet can make combatting such activity more challenging, failing adequately to address online illegal activity not only leads to grave societal harms, but also runs counter to the goal of an open and interoperable internet itself.

As an overall priority and guiding principle, COA urges NTIA to adopt as a central international internet policy priority for 2018 and beyond combatting online illegal activity that harms U.S. consumers, businesses, and societal interests and urging foreign governments and multilateral organizations to do the same. In particular, NTIA should promote, encourage and foster a wide range of internet intermediaries and platforms (both domestic and foreign) to take on greater responsibilities for identifying and removing clearly infringing content and associated illegal activity from their platforms and services, and adopting measures to prevent such infringing material from re-appearing. Doing so would bolster the internet's power as a vehicle for free expression, innovation and dissemination of creativity in a manner that respects the rights of creators, protects users and allows platforms to flourish under the rule of law.

Given COA's focus on the Domain Name System and the Internet Corporation for Assigned Names and Numbers ("ICANN"), we urge that NTIA take steps to enlist increased cooperation from domain name registrars and registries to suspend the domain names of websites that are engaged in clearly copyright infringing activity—as well as other clearly illegal activity. This should be accomplished by seeking respect for and enforcement of current contractual obligations of accredited registrars and registries, as well as voluntary measures. Furthermore, we encourage NTIA to maintain its strong support for accurate and publicly accessible WHOIS data and very much appreciate the clear and consistent statements made by Assistant Secretary Redl in this regard.[1]

We further support NTIA's work to continue to serve in a leadership role both within the ICANN Governmental Advisory Committee ("GAC") and in its own policy and diplomatic initiatives to resist applications and interpretations of the European Union's General Data Protection Regulation ("GDPR") and other privacy laws that do not strike a reasonable and appropriate balance between data privacy and the critical array of public interests—and indeed the stable and secure functioning of the internet—that rely on access to the full range of WHOIS data.

[1] *See, e.g., remarks of Assistant Secretary Redl at the State of the Net 2018 (January 29, 2018)* "The first [priority] is the preservation of the WHOIS service, which has become one of NTIA's most pressing issues related to ICANN." at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-state-net-2018 *; remarks of Assistant Secretary Redl at ICANN 61 (March 12, 2018)* "The United States will not accept a situation in which WHOIS information is not available or is so difficult to gain access to that it becomes useless for the legitimate purposes that are critical to the ongoing stability and security of the Internet." at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61 *; and remarks of Assistant Secretary Redl at the National Security Telecommunications Advisory Committee Meeting (May 17, 2018)* "GDPR is also threatening to upend the valuable WHOIS service . . . ." at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-national-security-telecommunications-advisory

SPECIFIC QUESTONS POSED BY NOI

I. The Free Flow of Information and Jurisdiction

COA supports the free flow of information and freedom of expression online. We note that rigorous enforcement of copyright online is perfectly consistent with—and in fact encourages—both the free flow of information and freedom of expression. Indeed, the U.S. Supreme Court has explicitly recognized "copyright itself to be the engine of free expression." Harper & Row v. Nation Enterprises, 471 U.S. 539, 558 (1985).

Unfortunately, copyright infringement is rampant online and continues to grow. As technology evolves, it takes on new forms from direct file downloads, to peer-to-peer file distribution, to illegal streaming services. Online infringement clearly harms U.S. copyright industries and legitimate online distribution services. But it also damages freedom of expression because it can destroy the livelihood of independent creators and upcoming artists and therefore their wherewithal to create and bring new works to the public.[2]

Beyond stifling freedom of expression and the free flow of information, online copyright piracy harms consumers and the public at large. Copyright itself is premised on the recognition that the ultimate beneficiary of copyright protections is the public, which benefits from the creative and cultural contributions that copyright encourages. In the context of online piracy, copyright infringement has been associated with a variety of harms, including identity theft, fraud, and exposure to malware. According to a 2015 study by the Digital Citizens Alliance, consumers are "28 times more likely to get malware from a content theft site than on similarly visited mainstream websites or licensed content providers."[3]

Therefore, we believe that online copyright piracy stands as one of the primary challenges—although certainly not the only challenge—to freedom of expression and the free flow of information online. Responding effectively to this challenge should be accorded a high priority in the U.S. government's international Internet policies.

In terms of the role of all stakeholders globally, and what NTIA can do, to help ensure the free flow of information and freedom of expression online, we urge that greater emphasis be placed on voluntary cooperation and voluntary measures to combat clear online copyright piracy. A specific example of such voluntary cooperation is the Trusted Notifier program entered into by the MPAA and two major domain name registries, Donuts and Radix. Under this arrangement, MPAA has referred websites involved in clear and pervasive copyright infringing activity to Donuts or Radix (after having attempted to obtain cooperation from the registrar and hosting provider) and where Donuts or Radix is the registry for the domain name under which the pirate website is operating. The registries then evaluate the sites and have suspended the domain names for violation of the registries' terms of use. The Trusted Notifier program has worked to the mutual satisfaction of both the IP rightsholders (here the MPAA as representative of its member companies) and the online intermediary/service provider (here the domain name registries).[4] Unfortunately, no other generic Top Level Domain ("gTLD") domain name registries have followed the cooperative and productive path undertaken by Donuts and Radix; similarly no gTLD registrars have entered into such voluntary arrangements. But the Donuts and Radix experiences prove that action by domain name registrars

[2] *See, e.g.:* https://www.forbes.com/sites/nelsongranados/2016/02/01/how-online-piracy-hurts-emerging-artists/#54b5cc697774

[3] *See:* https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf

[4] *See:* https://www.mpaa.org/press/one-year-later-trusted-notifier-program-proves-effective/

and registries to address copyright infringement and other clear abuses is eminently feasible and reasonable.

We would like to see NTIA promote this type of Trusted Notifier program with other major U.S. domain name registries and registrars, and similar efforts with other internet intermediaries, in order to more efficiently curb rampant online copyright piracy and therefore encourage freedom of expression online.

One of the most difficult challenges in enforcing copyrights online is the jurisdictional challenge and the fact that the internet is seamless and global. It is not uncommon for the hosting provider for a pirate website to be located on a different continent—let alone in a different country—from the website operator. Similarly, the domain name registrar and registry for the pirate website are often located in still other different countries. This is part of the reason why voluntary measures and cooperative arrangements between IP rightsholders and platforms/internet intermediaries are so important and should be promoted by governments. We are encouraged, for example, by the European Commission's recent Recommendation of March 1, 2018 on measures to effectively tackle illegal content online and its endorsement of trusted flagger arrangements, technological solutions and the adoption and sharing of best practices to tackle illegal content online.[5] We urge the United States government, and NTIA in particular, to undertake efforts to foster similar arrangements both at home and abroad.

II. Multistakeholder Approach to Internet Governance

COA will focus its replies to the questions concerning the multistakeholder approach to internet governance on ICANN, where COA has been actively engaged for nearly two decades. With respect to ICANN, we agree with the recent remarks made Assistant Secretary Redl at the ICANN 61 meeting in March 2018 "in advocating for, participating in and supporting the multistakeholder model of Internet governance." Equally, we support Assistant Secretary Redl's further statements that "ICANN can improve its policy development processes and bring greater predictability and transparency into its processes and actions." In addition, COA believes that substantial improvements can and should be made with respect to both accountability and enforcement by ICANN of its contractual obligations vis-à-vis domain name registrars and registries. While COA does not recommend that the IANA stewardship transition should be unwound, we think the multistakeholder model has fallen short in several critical respects in the case of ICANN, that ICANN itself has not been proactive in living up to commitments made during consideration of the IANA transition, and that substantial efforts must be undertaken to improve its efficacy and functioning.

A clear example of such a shortfall concerns the 2013 Registrar Accreditation Agreement ("RAA"). After extensive consultations and negotiations within the multistakeholder community, the RAA was adopted by ICANN as the new standard contract with its accredited domain name registrars. The RAA refers more explicitly than the prior agreement to the obligation of domain name registrars to undertake efforts to address clearly abusive uses of registered domain names. The RAA requires registrars to maintain an abuse contact to receive reports of illegal activity involving use of a domain name and obligates registrars to "investigate and respond appropriately" to abuse reports they receive from any third parties.[6] Another key provision of the RAA requires registrars to make

[5] *See in particular recitals 29 and 30 and paragraphs 25-28 of the Commission Recommendation at* https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[6] *See section 3.18.1 of the 2013 RAA at* https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

"commercially reasonable efforts" to ensure that registrants comply with their promises not to use their domain names "directly or indirectly" to infringe the legal rights of third parties.[7]

Taken together, these provisions were designed to—and should—provide an important avenue of redress against those who abuse gTLD domain name registrations to operate sites for pervasive copyright piracy or trademark counterfeiting, among other abuses and illegal activity. Unfortunately, in practice to date these provisions have yielded very little value.

COA members have brought to the attention of accredited domain name registrars dozens of domain names sponsored by those registrars associated with the operation of piracy websites dedicated to blatant infringement of copyrighted content, including music, movies, TV programming, software, videogames and books. In almost every case, the registrars failed to investigate or take any other action to deal with the flagrant infringing activity engaged in by their registrants using these domain names. In several instances, rightsholder organizations have then filed complaints with ICANN, fully documenting the refusal of accredited registrars to respond appropriately or meaningfully, and asking ICANN to enforce the relevant provisions of the RAA. Although fully capable and responsible for enforcing the RAA, ICANN's response has been to dismiss these complaints, telling the complainants only that the registrars have "responded appropriately."

Thus, even though these important RAA anti-abuse provisions were painstakingly arrived at via the multistakeholder process, they have not proven to be effective in practice as a result of the broad leeway afforded by ICANN to registrars and registry operators. This is particularly disappointing—and we believe unacceptable—in the area of copyright infringement, where an extraordinarily high level of international consensus exists and a consistent set of standards and legal principles are embraced by the global community about the fundamental nature and value of copyright and the need for protection against blatant infringement. This consensus and consistency are demonstrated by the 176 countries that are signatories to the Berne Convention for the Protection of Literary and Artistic Works ("Berne Convention") and the 162 countries that are signatories to the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPs"). Unless and until registrars begin to comply in good faith with the obligations that they voluntarily accepted when they signed the 2013 RAA, and unless and until ICANN undertakes meaningful and substantive action against those who will not comply based on a reasonable interpretation of the obligations in the contracts, these provisions will simply languish as empty words, and their potential to improve transparency, accountability and the rule of law in the Domain Name System ("DNS") will never be realized.

As COA stated in testimony before Congress in 2015, "the essence of the 'multistakeholder model' of DNS governance is the replacement of governmental regulation of a critical public resource with private contractual constraints and community oversight. This model only works when those contracts are strong and when they are vigorously and transparently enforced."[8] We encourage NTIA to continue to work with its fellow GAC members to improve transparency, accountability and effectiveness of ICANN in this area, particularly with respect to enforcement of existing contracts related to abuse complaints concerning copyright piracy.

A recent and equally significant shortcoming of the multistakeholder process within ICANN concerns changes undertaken to the WHOIS Registration Directory Service ("WHOIS") to comply with the GDPR.

---

[7] *See section 3.7.7 and 3.7.7.9 of the 2013 RAA at* https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

[8] See: https://judiciary.house.gov/wp-content/uploads/2016/02/05.13.15-Metalitz-Testimony.pdf

As NTIA is well aware, domain name registration information has been publicly accessible through WHOIS since the earliest days of the DNS, even predating the World Wide Web. Public access to WHOIS data is essential to the investigation and prompt resolution of instances of copyright piracy and trademark counterfeiting online. The investigation of virtually every such case involves the use of WHOIS data. WHOIS data is equally important to investigations of distribution of malware, cyberattacks, phishing and online frauds and illegal behavior of all kinds.

WHOIS data is essential to law enforcement, of course, but also to private parties such as copyright and trademark owners, whose independent enforcement of their rights allows law enforcement to conserve scarce resources. Indeed, virtually every internet user benefits from publicly accessible WHOIS data. WHOIS provides greater transparency, so that end users know more about the parties with whom they – or their children – are interacting online. This is a fundamental prerequisite to building public confidence and accountability in the online ecosystem and economy.

For many years, WHOIS has been the subject of re-examination and discourse within the ICANN multistakeholder community, partially although certainly not exclusively, due to concerns with privacy laws of some countries. In 2012, an Expert Working Group was formed to help redefine the purpose and provision of WHOIS data. That Expert Working Group released its Recommendations for public comment in 2013 and issued a comprehensive, 166 page Final Report in June 2014.[9] A Policy Development Process ("PDP") called "the Next Generation gTLD RDS to Replace WHOIS PDP Working Group" was then launched in 2015 to formulate new WHOIS policy and a new registration directory service to take account of a wide range of issues, including privacy law issues. Unfortunately, the PDP became mired in contentious debate, and being unable to reach consensus on fundamental issues, let alone fulfill its mission, the PDP has now been suspended. While this is partly a result of intervening events (such as GDPR compliance, discussed below), the inability to make meaningful progress after more than two years of discussion represents a failure of the multistakeholder model to address and resolve key policy issues, to the significant detriment of U.S. law enforcement entities and inflicting harm on U.S. business interests that the broader U.S. Department of Commerce is charged to protect.[10]

With the May 25, 2018 effective date of the GDPR looming, ICANN org took upon itself to propose a Temporary Specification for WHOIS, which the ICANN Board adopted on May 17, 2018.[11] While ICANN org continually stated that its goal was to ensure compliance with the GDPR "while maintaining the existing WHOIS system to the greatest extent possible,"[12] the terms of the Temporary Specification fly in the face of that statement.

The Temporary Specification eradicates the essential value of WHOIS in aspects not mandated by the GDPR as follows:

1. It applies to registrations of legal persons as well as natural persons, even though the privacy protections of the GDPR only apply to natural persons.

---

[9] *See*: https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf

[10] Similarly, ICANN's failure to implement the consensus policy unanimously adopted by its Board in 2016 regarding the accreditation of privacy/proxy registration services significantly harms the vital interests of U.S. intellectual property rights holders, business interests generally, and consumers. While the compelling need to bring consistency and predictability to the operation of these services is broadly recognized, and the adopted policy represents a balanced compromise among all the competing interests, the implementation process has been frozen in place for the past many months.

[11] *See*: https://www.icann.org/resources/pages/gtld-registration-data-specs-en

[12] *See, e.g.*: https://www.icann.org/news/blog/data-protection-privacy-update-seeking-input-on-proposed-interim-model-for-gdpr-compliance

2. It invites registrars and registries to apply its restrictions globally and to all registrations, even those that lack any point of attachment to the European Economic Area and thus fall outside the jurisdictional reach of the GDPR.
3. It requires the redacting of the most important elements of WHOIS data without appropriately balancing public and legitimate interests against privacy interests as provided under the GDPR. In particular, the Temporary Specification fails to provide public access to the registrant's actual email address as supplied by the registrant to the registrar and then verified by the registrar. The redaction of the registrant's e-mail address pursuant to the Temporary Specification was made despite precise and forceful recommendations to the contrary from several contingents of the multistakeholder community, as well as the GAC and the European Commission itself. For law enforcement, cybersecurity, consumer protection and IP rights protection, the registrant's e-mail address is the most important WHOIS data element because it is usually the most accurate data point and it also allows investigators to link domains and actors together that are involved in illegal and abusive activity.
4. Although the Temporary Specification, consistent with GDPR principles, requires registrars and registries to provide reasonable access to non-public WHOIS data to third parties with legitimate interests except where such interests are overridden by the interests or fundamental rights and freedoms of the registrant, it gives no guidance or specifics whatsoever as to how that standard should be implemented or as to how access should be granted.

In adopting the Temporary Specification, the ICANN Board (by its own admission) acted inconsistently with the consensus advice of the GAC and the guidance from key stakeholder groups including the Security and Stability Advisory Committee, the Intellectual Property Constituency and the Business Constituency. Instead, ICANN org and the Board seem to have to paid attention only to the views of the registrars and registries. Since the adoption of the Temporary Specification, fragmentation within the WHOIS system abounds. No uniform framework exists for access to non-public WHOIS data and registrars have been left to their own devices to develop policies and procedures—or not—for such access. The result has been confusion and, far beyond anything GDPR requires, a nearly complete shut-down of any legitimate access to all WHOIS data that the Temporary Specification has identified and required to be made non-public.

Less than two months ago, 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.[13] 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 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."[14]

To date, the implementation of the Temporary Specification has seriously eroded timely access to WHOIS information to the detriment of not only efforts to investigate botnets and other

[13] *See*: Report https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf
[14] Ibid., 40

cybersecurity threats, but also all other online enforcement efforts, including intellectual property rights infringements.

COA deeply appreciates NTIA's ceaseless work and leadership with respect to ICANN matters, particularly in its role as the U.S. government representative to the GAC. We encourage NTIA to continue its leadership role to ensure that public interests are served and well-represented. Going forward, we suggest the following priorities for NTIA within ICANN and the GAC:

1. Continue to press the ICANN staff and the ICANN Board to adopt and fully implement as soon as possible the GDPR and WHOIS consensus advice that the GAC delivered in its ICANN 61 San Juan Communique[15];

2. Continue to support and press for the adoption of a workable, efficient and uniform accreditation and access process for non-public WHOIS data as an amendment to the Temporary Specification and/or via the Expedited Policy Development Process ("EPDP") on the Temporary Specification;

3. Ensure that GAC representatives participate and embrace an active leadership role in the EPDP on the Temporary Specification;

4. Press ICANN org to complete the final stages of the implementation review process of the Privacy/Proxy Services Accreditation policy and to stop delaying the implementation of this critical policy that was approved by the ICANN Board in August 2016; and

5. Engage with GAC and ICANN org to address ICANN's lack of meaningful enforcement of the anti-abuse provisions of the RAA.

In addition to its work with respect to ICANN and the GAC, we urge NTIA to help educate domestic lawmakers on the importance of WHOIS and the need for action, including potential U.S. legislation, to ensure continued access to critical WHOIS data for the protection of public and other legitimate interests and to prevent misapplications of privacy laws, such as the GDPR, to serve as a cover for illegal activity and abuse. Congress and the Administration should work together to take whatever practical steps are available to ameliorate the adverse impact on American consumers, intellectual property right holders, businesses and other internet users of ICANN's unwise decision to reduce WHOIS access far below what GDPR requires. Similarly, we encourage NTIA and others in the U.S. government to work with the EU Commission and European governments on potential legislative or regulatory solutions to establish the correct balance of public and privacy interests with respect to WHOIS data. Finally, we suggest that NTIA actively engage with leading U.S. registries and registrars to encourage them to engage in voluntary initiatives with copyright owners, such as the successful Trusted Notifier program described earlier in these comments.

III. Privacy and Security

One need look no further than the above-referenced recent Report on Enhancing the Resilience of the Internet and Communications Ecosystems Against Botnets and Other Automated, Distributed Threats to appreciate how dramatically cybersecurity threats are harming commerce and consumers, both domestically and internationally. As the Report notes, "[Distributed denial of service attacks] have grown in size to more than one terabit per second, far outstripping expected

[15] *See*: https://www.icann.org/en/system/files/correspondence/gac-to-icann-15mar18-en.pdf

size and excess capacity."[16] Other reports confirm the disturbing and damaging increase in cybersecurity threats and abuse. For example, the 2017 Phishing Trends & Intelligence Report notes that "phishing volume grew by an average of more than 33% across the five most-targeted industries [financial institutions, cloud storage/file hosting services, webmail/online services, and ecommerce companies]."[17] As noted earlier in these comments, websites devoted to copyright piracy are far more likely to deliver malware and other cyberabuse than non-infringing websites.[18] Thus, a close nexus exists between cybersecurity threats and other illegal activity online, including copyright infringement.

In this context, a reasonable and prudent balance must be struck between protecting against cybersecurity threats and online illegal activity and protecting privacy rights. Indeed, applying extreme interpretations of privacy rights in the online environment may actually result in increased theft and abuse of personal information.

COA believes that ICANN has strayed far from the mark in achieving a reasonable and prudent balance in its Temporary Specification. We encourage NTIA to educate policy makers at home and abroad about the real and growing threats posed by botnets, malware, phishing as well as other online illegal activity including trafficking in child abuse images and videos, copyright infringement and counterfeit goods. Protection of personal data is important, and people's privacy rights clearly need to be protected online and offline. But a proportionate balance must be found so that protection of privacy does not thwart the goal of achieving a more safe and secure internet and information economy.

CONCLUSION

COA thanks NTIA for the opportunity to comment on these important issues and priorities. We would be happy to answer any further questions you may have about this submission and to provide any additional information.

Respectfully submitted,

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

[16] Report, 5.
[17] *See*: https://info.phishlabs.com/2017-phishing-trends-and-intelligence-report-pt
[18] *See footnote 3 and associated text*.