Recording Industry Association of America Response to
National Telecommunications and Information Administration
Request for Comments on the
Introduction of Accountable Measures Regarding Access to Personal Information of .us Registrants
Docket No. 2023-0006
230412-0099
RIN 0660-XC058

Submitted via regulations.gov

May 31, 2023

The Recording Industry Association of America ("RIAA") welcomes this opportunity to provide comments to the National Telecommunications and Information Administration ("NTIA") in response to its request for comments on the introduction of accountable measures regarding access to personal information of .us registrants ("RFC").

The RIAA is the trade organization that supports and promotes the creative and commercial vitality of music labels in the United States, the most vibrant recorded music community in the world. Our membership – which includes several hundred companies, ranging from small-to-medium-sized enterprises to global businesses – creates, manufactures, and/or distributes sound recordings representing the majority of all lawful recorded music consumption in the United States. In support of its mission, the RIAA works to protect the intellectual property and First Amendment rights of artists and music labels; conducts consumer, industry, and technical research; and monitors and reviews state and federal laws, regulations, and policies.

Human creative expression is at the core of our members' businesses, and it is vital to our nation's culture and economy. The U.S. boasts over one million revenue-generating sound recording artists and songwriters.[1] Overall, the music industry contributes $170 billion to the nation's economy, supports 2.47 million jobs, and accounts for over 236,000 businesses in the United States.[2] For every dollar of direct revenue within the U.S. music industry, an additional

[1] Source: https://50statesofmusic.com/?USimpact.
[2] Source: https://50statesofmusic.com/?USimpact.

50 cents is created in an adjacent industry to the U.S. economy.[3] More broadly, in 2021, the value added to the GDP by the core copyright industries, of which we are a part, exceeded $1.8 trillion dollars, accounting for 7.76% of the U.S. economy.[4]

Ensuring a healthy Internet ecosystem is vital for the music community (as well as others in core copyright industries). The great majority of our members' revenues are derived from the Internet. In 2022, nearly 90% of recorded music revenues in the U.S. came from digital sources, with digital streaming of sound recordings accounting for 84% of U.S. recorded music revenues.[5] The number of paid subscriptions for on-demand music services grew 10% to reach a new high, averaging 92 million subscriptions in 2022. At the same time, however, theft of our members' music on the Internet remains a significant problem.

Our ability to enforce our members' rights online are significantly diminished when the contact information for a domain name registrant is not readily available, transparent or accurate. This problem has become more severe since ICANN implemented a policy in 2018 in response to the EU's General Data Protection Directive (GDPR) - and failed to implement a privacy/proxy policy - with generic top-level domains (gTLDs) that, as implemented by most registrars, makes the ability to obtain accurate registrant data for intellectual property enforcement purposes virtually non-existent.

We have seen much less copyright infringement on sites with .us domains than on those in the gTLD space. For example, as shown in the table below, the number of domains we have noticed infringing our members' works is exponentially lower on .us (less than 100 in both time periods noted) than the number of infringing domains noticed on .com (in the thousands for both periods noted).

TLD	*No. of infringing domains noticed during the period 2013-2017*	*No. of infringing domains noticed during the period 2018-2022*	*% difference in infringing domains between these two time periods*
.us	97	75	-22.6%
.com	4843	6496	+34.1%

This is true for both the five-year period from 2013 to 2017 (when privacy/proxy services were permitted in connection with registration of domains on .com), as well as the subsequent five-year period from 2018 to 2022 (when, in addition to permitting privacy/proxy services, much of the registrant information was redacted from public inspection for .com domains). Moreover,

[3] Source: The U.S. Music Industries: Jobs & Benefits, the 2020 Report, prepared by Economists, Inc. for the Recording Industry Association of America (December 2020), available at https://www.riaa.com/wp-content/uploads/2021/02/The-U.S.-Music-Industries-Jobs-Benefits-2020-Report.pdf.

[4] Stoner, Robert et al., "IIPA, Copyright Industries in the U.S. Economy, 2022 Report," Secretariat Economists, prepared for the International Intellectual Property Alliance, Dec. 2022, p. 8, available at https://www.iipa.org/files/uploads/2022/12/IIPA-Report-2022_Interactive_12-12-2022-1.pdf.

[5] Source: RIAA, see https://www.riaa.com/wp-content/uploads/2023/03/2022-Year-End-Music-Industry-Revenue-Rep; ort.pdf.

when we compare the difference in the number of infringing domains over these two time periods, which roughly translate to the five years before and after ICANN's 2018 implementation of a policy to restrict WHOIS access for gTLDs, we see a 22.6% decrease in infringing domains on .us, versus a 34.1% increase in infringing domains on .com. We suspect that these differences in the incidence of infringing domains is in part due to .us's long-standing policies to prohibit privacy/proxy registrations for .us domains and to keep registrant information publicly available for inspection.

The problems created by the lost access to registrant data affect not only intellectual property rights holders, but also law enforcement, civil agencies charged with protecting against consumer fraud, cybersecurity, and other forensic investigators who used registrant data to guard and fight against various online harms. The Anti-Phishing Working Group, Inc. (APWG) reported that "2022 was a record year for phishing, with the APWG logging more than 4.7 million attacks. Since the beginning of 2019, the number of phishing attacks has grown by more than 150% per year." [6] In the 4th quarter of 2022 alone, the APWG reported that 1,350,037 unique phishing web-sites (attacks) had been detected.[7] By comparison, in the 4th quarter of 2017, when registrant data was more publicly available, the number of phishing web-sites (attacks) detected was only 180,757.[8]

In 2021, the APWG and the Messaging Malware Mobile Anti-Abuse Working Group (M[3]AAWG) conducted a joint survey of their members to gauge the impact of ICANN's implementation of GDPR. They found that "respondents report that changes to WHOIS access following ICANN's implementation of the EU GDPR, the Temporary Specification for gTLD Registration Data (Temporary Specification, adopted in May 2018), continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyberattack."[9]

Conversely, while we have heard of anecdotal evidence of harm to registrants generally, we don't know of any documented, verifiable, widespread, pervasive harm to .us registrants caused by publicly available registrant data. In fact, in the RFC, NTIA asks for illustrative examples of harm, suggesting that NTIA does not have evidence supporting a change to .us current practices.

---

[6] APWG, "Phishing Activity Trends Report," 4th Quarter, 2022," May 9, 2023, p. 2, available at https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf?_gl=1*1ake3yk*_ga*MzMzNzI2NDMxLjE2ODQ3NjQxMDA.*_ga_55RF0RHXSR*MTY4NDc2NDA5OS4xLjEuMTY4NDc2NjIzMi4wLjAuMA.

[7] Id at p. 3.

[8] APWG, "Phishing Activity Trends Report 4th Quarter 2017," May 15, 2018, available at https://docs.apwg.org//reports/apwg_trends_report_q4_2017.pdf?_gl=1*hli9i4*_ga*MzMzNzI2NDMxLjE2ODQ3NjQxMDA.*_ga_55RF0RHXSR*MTY4NDc2NDA5OS4xLjEuMTY4NDc2NjIzMi4wLjAuMA.

[9] M3AAWG and APWG, "ICANN, GCPR, and the WHOIS: A Users Survey – Three Years Later", June 2021, p. 3, available at https://docs.apwg.org/reports/M3AAWG_APWG_WHOIS_User_Survey_Report_2021.pdf?_ga=2.68048721.1130029619.1639836752-1478579126.1639836751&_gl=1*1p7o0wj*_ga*MzMzNzI2NDMxLjE2ODQ3NjQxMDA.*_ga_55RF0RHXSR*MTY4NDkzNDQzNy4zLjAuMTY4NDkzNDQzNy4wLjAuMA.

Given the steep rise of cyber problems since the WHOIS data for gTLDs was masked, and the challenges such masking has caused to those combatting those problems, we don't understand why .us would change its current policies. ***Accordingly, the current system of access to usTLD domain name registration data should remain unchanged, and we do not support efforts to create unnecessary gates around registrant data.***

Moreover, any efforts to mask domain name registrant data on the .us ccTLD would be contrary to the long-standing policy of the United States. Current .us policy prohibits privacy/proxy registrations, on the understanding that transparency of registrants so they can be held accountable for their actions with a .us domain is an important policy objective. Further, as noted in a March 12, 2018 speech by then-NTIA administrator David Redl, the "United States will not accept a situation in which WHOIS information is not available or 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."[10] In addition, Congress has held multiple inquiries into the accuracy and availability of registrant data, showing the U.S. government's interest in and commitment to ensuring that transparency and accountability exist in the DNS system.[11] Indeed, the U.S. has further expressed this commitment in several of its trade agreements, which include provisions calling for online public access to a reliable and accurate database of contact information on domain-name registrants.[12] This strong U.S. policy of transparency and accountability in the domain name system further cautions against making any changes to the .us registration data system.

While we counsel against changing the current system of access to the usTLD domain name registration system for the reasons set forth above, if, nonetheless, NTIA moves forward with masking usTLD domain name registration data, we offer the following additional comments. First, intellectual property (IP) rights holders should be given free, immediate access to registrant data if requested to protect their rights (whether copyright, trademark, state intellectual property rights, or otherwise) based on their assertion that they are seeking the information in connection with enforcement of their rights (as well as cybersecurity

---

[10] Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61, San Juan, Puerto Rico, March 12, 2018, available at https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61.

[11] See, e.g., Hearing of the Subcommittee on Courts, the Internet and Intellectual property of the House Judiciary Committee titled "WHOIS Database: Privacy and Intellectual Property Issues" on July 12, 2001; Hearing of the Subcommittee on Courts, the Internet and Intellectual property of the House Judiciary Committee titled "Accuracy and Integrity of the Whois Database" on May 22, 2002; Hearing of the Subcommittee on Courts, the Internet and Intellectual Property of the House Judiciary Committee titled "Internet Domain Name Fraud – The U.S. Government's Role in Ensuring Public Access to Accurate Whois Data" on September 4, 2003; Hearing of the Subcommittee on Financial Institutions and Consumer Credit of the House Financial Services Committee titled "ICANN and the Whois Database: Providing Access to Protect Consumers from Phishing" on July 18, 2006; Hearing of the Subcommittee on Communications and Technology of the House Energy and Commerce Committee titled "National Telecommunications and Information Administration Reauthorization act of 2018" on June 26, 2018.

[12] See, e.g., the Australia Free Trade Agreement, Section 17.3.2, the Korea Free Trade Agreement, Section 18.3.2, etc.

investigators, law enforcement, civil agencies, and any others with a legitimate need for the data). Second, such a system should distinguish between personal and non-personal registration data. For example, if the registrant is a corporation, all of the registrant information should be publicly available, including the contact information for the registrant if the registrant chooses to list an employee as the contact. Third, the usTLD should implement a strong due diligence checks / know your customer requirements of all registrants to ensure the information they provide is accurate, as has been recommended by the European Commission.[13]

* * *

We thank NTIA for the opportunity to share these views on policies for .us.

[13] European Commission, "Study on Domain Name System (DNS) Abuse," January 2022, available at https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1.