



Comments of the Recording Industry Association of America on the usTLD Stakeholder Council  
Statement of USTLD Recommendations for Privacy Policies

March 28, 2021

The Recording Industry Association of America (RIAA) welcomes this opportunity to comment on the usTLD Stakeholder Council (Council) Statement of USTLD Recommendations for Privacy Policies, and to respond to the questions posed by the Council.<sup>1</sup>

The RIAA is the U.S. trade organization representing the major recorded music companies. RIAA's members create, manufacture, or distribute sound recordings representing approximately 85 percent of all legitimate 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.

Ensuring a healthy Internet ecosystem is vital for RIAA's members. The great majority of our members' revenues are derived from the Internet. In 2020, nearly 90% of sound recording revenues in the U.S. came from digital sources, with 83% of recorded music revenues coming from streaming sound recordings. At the same time, however, theft of our members' music on the Internet remains rampant. Our efforts to enforce our members' rights online are significantly diminished when the contact information for a domain name registrant is not transparent. Moreover, users of sites that engage in infringement are often harmed as well by identity theft scams, malware, and other malfeasance occurring via the site.<sup>2</sup>

We have seen much less copyright infringement on sites with .US domains than on top-level domains that permit privacy/proxy registrations, or which permit redaction of public domain name registrant information. We suspect that this is in part because of .US's long-standing policy to prohibit privacy/proxy registrations for .US domains.

Accordingly, we **do not support** the implementation of a policy to allow for privacy services for .US domain name registrants, nor do we support the implementation of private services to all domain holders regardless of commercial status. While we appreciate that there may be some lawful uses for

---

<sup>1</sup> See <https://www.about.us/policies/ustld-stakeholder-council/ustld-privacy-recommendation>.

<sup>2</sup> See, e.g., Janveva et al, Whitehall Report 4-20: Taking the Profit out of Intellectual Property Crime: Piracy and Organized Crime, Royal United Services Institute for Defence and Security Studies (March 2021), available at [https://rusi.org/sites/default/files/whr\\_ip\\_crime\\_web\\_version.pdf](https://rusi.org/sites/default/files/whr_ip_crime_web_version.pdf); Digital Citizens Alliance, *Digital Bait*, available at <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf>.

privacy/proxy services, on balance, the public interest in transparency in knowing “who is behind the screen” with respect to a domain and the accountability that transparency provides to prevent all types of harm (including intellectual property infringement, fraud, cybersecurity risks, etc.) significantly outweighs the concerns raised in the Council’s USTLD Recommendations for Privacy Policies.

Moreover, any efforts to obfuscate or mask domain name registrant data on the .US ccTLD would be contrary to the long-standing policy of the United States. 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.”<sup>3</sup> 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.<sup>4</sup> 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.<sup>5</sup>

For all of these reasons, the .US domain should continue to prohibit the use of privacy/proxy registrations, and the Council’s usTLD Recommendations for Privacy Policies should be rejected.

---

<sup>3</sup> 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>.

<sup>4</sup> 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.

<sup>5</sup> See, e.g., the Australia Free Trade Agreement, Section 17.3.2, the Korea Free Trade Agreement, Section 18.3.2, etc.