

Nov. 9, 2018

The National Music Publishers' Association and the Recording Industry Association of America
Response to
National Telecommunications and Information Administration
Request for Comments re:
Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780-8780-01
Submitted via email to privacyrfc2018@ntia.doc.gov

The National Music Publishers' Association (NMPA) and the Recording Industry Association of America (RIAA) welcomes the opportunity to respond to the National Telecommunications and Information Administration (NTIA) request for comments on ways to advance consumer privacy while protecting prosperity and innovation.

Founded in 1917, NMPA is the principal trade association representing the U.S. music publishing and songwriting industry. NMPA protects and advances the interests of music publishers and songwriters in matters relating to both the domestic and global protection of music copyrights. NMPA represents publishers and songwriters of all catalog and revenue sizes, from large international corporations to small businesses and individuals. Taken together, compositions owned or controlled by NMPA members account for the vast majority of the market for musical composition licensing in the U.S. NMPA aims to protect its members interests through legislative, litigation and regulatory efforts, by representing our members in industry negotiations and in maintaining an antipiracy program to combat unauthorized uses of its members works on unlicensed websites, applications and various online platforms.

The RIAA is the trade association that supports and promotes the financial vitality of the major record companies. Its members comprise the most vibrant record industry in the world, investing in great artists to help them reach their potential and connect to their fans. Nearly 85% of all legitimate recorded music produced and sold in the United States is created, manufactured or distributed by RIAA members. 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.

Music is a vital part of our nation's culture, and drives consumers to various online platforms to access, engage with and consume the music they love. Consider, for example, that in the first half of 2018, 87% of U.S. sound recording revenues came from digital sources, with 75% from various forms of streaming.¹ Music also helps drive various Internet business and Internet growth generally. For example, music videos are the biggest content genre on YouTube, with

¹ Source: RIAA - See <https://www.riaa.com/wp-content/uploads/2018/09/RIAA-Mid-Year-2018-Revenue-Report-News-Notes.pdf>.

1.1 trillion streams in 2017 globally.² Music has also driven smart speaker adoption and online social media engagement.³ In fact, 4 of the 5 largest U.S. technology companies have licensed music for use on their platforms by our music's fans.⁴ Unfortunately, several rogue infringing services attempt to capitalize on our Nation's love for music by using music as the lure to get consumer eyeballs to their sites for their own monetization purposes. The distinctive relationship of music to both consumers and to online platforms that use music to engage consumers (whether those platforms are licensed or infringing), gives us a unique and important perspective in considering a risk-based approach to online consumer privacy.

In considering any risk-based approach to privacy, a first principle must be that there is transparency around who is engaging the consumer online – i.e., who is on the other side of the screen. If the one on the other side of the screen is an entity, that entity's name, physical address, email address and other contact information must be disclosed and easily accessible, both on the website itself, and also on other records, such as the domain name registration record for the domain associated with the website.

To the extent the website operator/domain name registrant is an individual, a risk-based approach to privacy demands that one consider the risk of publication or disclosure of that individual's contact information in relation to the website/domain name versus the risks to consumers, the public and others that may be harmed by the activities engaged in or facilitated via the site/domain name in question. These risks could include the site operator/registrator's collection and use of users' personal information or the operator/registrator's activities on the site that potentially harm others, whether in terms of harm to consumers, cyberthreats, fraud, violation of third party rights or other harm or illegality.

Where the website operator/domain name registrant is collecting personal information about users of the site/domain, it seems obvious that the operator's/registrator's contact information, including name, physical address, email address and possibly other contact information must be disclosed publicly, so that consumers engaging with the site know who is collecting information about themselves, and how to contact them. Even if the website operator/domain name registrant is not collecting personal information about its users, the risk to consumers and third parties from activities occurring on or via the site must be considered, and users' need for transparency to avoid and mitigate harms from those activities should outweigh the privacy risks to the individual website operator/domain name registrant. Quite frankly, in either of these cases, the website operator/domain name registrant shouldn't be treated as a consumer at all, as that person's activities in relation to operating the site/using the domain extend beyond that of a mere consumer.

² Source: Media Research - See <https://www.midiaresearch.com/blog/state-of-the-youtube-music-economy-2-0-a-turning-point-for-all-parties/>.

³ See RIAA comments to NTIA NOI re: International Internet Policy Priorities dated July 17, 2018, Docket No. 180124068-8068-01.

⁴ Id.

Consider our experience as one example in this context. The music industry has suffered significantly from online copyright infringement, and users of these infringing sites are often harmed as well by identity theft scams, malware and other malfeasance occurring via the site.⁵ Our efforts to enforce our rights online are significantly diminished when the contact information for the site operator/domain name registrant is not transparent. This harms not only our efforts to deter infringing activity, it also limits innovation by our members and by licensed services by redirecting revenue that could otherwise go to innovative activity, and ultimately harms consumers.

We hope that policymakers will continue to learn from our experience, and develop more mature, nuanced policies that reconcile and balance the various interests online to create a safe, secure and vibrant Internet ecosystem, not only with respect to domain name registrant data, but also more broadly when considering the various players in the music ecosystem and the consumers desires in that ecosystem. In such an ecosystem, transparency is vital, along with an appropriate balancing of the various risks from lawful and unlawful activities that occur online. Privacy policy concerns are important but are only one of several important policy concerns that impact our Nation's engagement online and our digital policy agenda. As NTIA continues to consider an appropriate risk-based privacy regime, we encourage NTIA to look to policies that advance the concept of reasonable Internet responsibility and accountability at every level. This concept of responsibility and accountability should not only apply to reasonable expectations of privacy, depending upon the context, but also to reasonable expectations of transparency and accountability to the general public when website operators/domain name registrants or their users engage in invasive or harmful behavior. Only a risk-based approach can ensure that we can move nimbly to protect not only our music consumers, but also our industries and the general public when they are threatened online as well.

* * *

Thank you for the opportunity to submit our comments on this important topic. We look forward to working with NTIA on further developing its risk-based approach to consumer privacy.

⁵ See, e.g., Digital Citizens Alliance, *Digital Bait*, available at <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf>.