Comments of the American Association of Independent Music, the National Music Publishers' Association, and the Recording Industry Association of America on the National Institute of Standards and Technology Request for Information Related to NIST's Assignments under Sections 4.1, 4.5, and 11 of the Executive Order Concerning Artificial Intelligence

Docket No. NIST-2023-0009

Delivered via regulations.gov

February 2, 2023

The American Association of Independent Music, the National Music Publishers' Association, and the Recording Industry Association of America welcome this opportunity to provide comments to National Institute of Standards and Technology ("NIST") on its Request for Information Related to NIST's Assignments under Sections 4.1, 4.5, and 11 of the Executive Order Concerning Artificial Intelligence ("RFI").

I. Introduction

Who We Are. The American Association of Independent Music ("A2IM") is a 501(c)(6) not-for-profit trade organization headquartered in New York City that exists to support and strengthen the independent recorded music sector and the value of recorded music copyrights. Membership currently includes a broad coalition of hundreds of independently-owned American music labels. A2IM represents these independently-owned small and medium-sized enterprises' (SMEs) interests in the marketplace, in the media, on Capitol Hill, and as part of the global music community. In doing so, it supports a key segment of America's creative class that represents America's diverse musical and cultural heritage.

The National Music Publishers' Association ("NMPA") is the principal trade association representing the U.S. music publishing and songwriting industry. 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 United States. NMPA protects and advances the interests of music publishers and songwriters in matters relating to both the domestic and global protection of music copyrights before the legislative, judicial, and executive branches of the U.S. government.

The Recording Industry Association of America ("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 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.

Human creative expression is at the core of our members' businesses and is vital to our nation's culture and economy. In 2021, the value added to the GDP by the total copyright industries, of which we are a vital part, exceeded $2.9 trillion, accounting for 12.52% of the U.S. economy.[1] In addition, the total copyright industries employed nearly 16.1 million workers in 2021, accounting for 8.14% of all U.S. employment.[2] The music industry itself creates jobs and boosts the economy in all 50 states.[3] At the core of all this activity is the creativity of sound recording artists, songwriters, musicians, producers, recording engineers, and countless other participants in the music industry that bring music to life. As discussed below, artificial intelligence ("AI") has the potential to both significantly increase creators' ability to express themselves creatively and to significantly harm them and rightsholders through the unethical development and deployment of AI systems that unfairly exploit their expression or identity.

Core Principles. The Administration has made it clear that AI development should be done in a manner that is ethical, lawful, trustworthy, and safe, and that protects human rights. As the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence makes clear, the Administration "places the highest urgency on governing the development and use of AI safely and responsibly."[4] According to the White House, "[t]he important progress [of AI automated systems] must not come at the price of civil rights or democratic values."[5] Such respect for civil rights and democratic values necessarily includes respecting the rights of creators, performers, and other rightsholders in their creations, identities, and dignity.

The G7 has espoused similar views. On October 30, 2023, the Leaders of the G7 agreed on the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System, which provide that organizations should "implement appropriate data input measures and protections for personal data and intellectual property," further noting that "[a]ppropriate transparency of training datasets should also be supported and organizations should comply with legal frameworks." [6] They also agreed on the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, which further encourages such

---

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

[2] *Id*.

[3] 50 States of Music, https://50statesofmusic.com/.

[4] Exec. Order No. 14110, 88 Fed. Reg. 75191 (Nov. 1, 2023) (hereinafter "Executive Order").

[5] *See* The White House, Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights*, Oct. 4, 2022, available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/. *See also* the statement from the National Telecommunications and Information Administration ("NTIA") that it desires to develop AI accountability policies that can demonstrate "that AI systems are legal, effective, safe and otherwise trustworthy." 88 Fed. Reg. 22433 (Apr. 13, 2023).

[6] *See Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system*, ¶ 11, Oct. 30, 2023, available via https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system.

organizations to "implement appropriate safeguards, to respect rights related to privacy and intellectual property, including copyright-protected content." [7]

We agree that the development and deployment of AI systems should be done responsibly, ethically, and with respect for the artists, creators, and performers who have shaped our history and will chart the next chapters of human experience. At its core, we believe that the approach to responsible AI innovation and deployment requires a human-centric approach.

That is why we, along with more than 600 other entities, have signed onto the Human Artistry Campaign.[8] The Human Artistry Campaign calls for policy makers, AI developers, and those that deploy AI to take into account the following principles:

(i) technology has long empowered human expression, and AI will be no different;
(ii) human created works will continue to play an essential role in our lives;
(iii) use of copyrighted works and the use of voices and likenesses of professional performers requires authorization and free-market licensing from all rightsholders;
(iv) governments should not create new copyright or other IP exemptions that allow AI developers to exploit creations without permission or compensation;
(v) copyright should only protect the unique value of human intellectual creativity;
(vi) trustworthiness and transparency are essential to the success of AI and protection of creators; and
(vii) creators' interests must be represented in policy making.[9]

With these principles in mind, and in consideration of how the RFI relates to generative AI and the creation, use, and exploitation of music, we offer the following comments.[10]

---

[7] *See Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems*, ¶ 11, Oct. 30, 2023, available via https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems.

[8] *See* https://www.humanartistrycampaign.com/.

[9] *Id.*

[10] In addition to the comments below, we encourage NIST to review the following filings the music sector has made with NIST, National Telecommunications and Information Administration (NTIA), Office of Science Technology and Policy (OSTP), and the Copyright Office as they relate to the issues raised in the RFI: (a) Jan. 31, 2022 comments in response to NIST request for information regarding a Study to Advance a More Productive Tech Economy, Docket No. 21116-0234, and the Sept. 15, 2021, Apr. 29, 2022, and Sept. 29, 2022 comments in response to NIST requests concerning the artificial intelligence risk management framework, Docket No. 210726-0151, available at https://www.regulations.gov/comment/NIST-2021-0007-0033, https://www.nist.gov/system/files/documents/2021/09/17/ai-rmf-rfi-0119.pdf, https://www.nist.gov/system/files/documents/2022/05/19/Recording%20Industry%20Association%20of%20America.pdf, and https://www.nist.gov/system/files/documents/2022/11/16/Recording%20Industry%20Association%20of%20America%20%28RIAA%29.pdf (collectively the "NIST Comments"); (b) June 12, 2023 comments in response to NTIA AI Accountability Policy Request for Comment, Docket No. NTIA-2023-0005, available at https://www.regulations.gov/comment/NTIA-2023-0005-1277 ("NTIA Comments"); (c) July 7, 2023 comments in response to the OSTP Request for Information on National Priorities for Artificial Intelligence, Docket No. OSTP-TECH-2023-0007, available at https://www.regulations.gov/comment/OSTP-TECH-2023-0007-0231 ("OSTP Comments"); and (d) the Oct. 30, 2023 and Dec. 6, 2023 comments to the Copyright Office in the Matter of

II. Comments

1. *Developing Guidelines, Standards, and Best Practices for AI Safety and Security with a Focus on Generative AI*

Focus on Human Rights, including Copyright. As NIST develops its guidelines, standards, and best practices concerning generative AI, NIST should focus on protecting and promoting human rights, including copyright and rights to one's identity and dignity. Referenced in the RFI, the Administration envisions "a future where AI is used to advance human rights and human dignity."[11] Human creative expression, the bedrock of the music industry, is enshrined as a human right in the U.N. Universal Declaration of Human Rights,[12] as well as being protected by our Nation's Constitution[13] and the U.S. Copyright Act.[14] Human rights and human dignity also require that a person have control over the use of their name, image, voice, and likeness.[15] We appreciate that NIST has acknowledged the importance of intellectual property, including name, image, voice, and likeness rights, and the need to consider the risks associated with infringement of those rights in its AI Risk Management Framework ("AI RMF").[16] As discussed below, the need to address these risks is even greater in the generative (as compared to non-generative) AI context.

Impact of Generative AI on the Music Community. As with other new technologies, the music community lives at the forefront of, and is building and inspiring, evolutions in generative AI technology. AI already is playing a role as a tool to assist the creative process and will increasingly do so, allowing for a wider range of people to express themselves creatively. Generative AI has been used for lyrics and composition ideation, beat making, and musical arrangement, as well as for mixing and mastering sound recordings. It has helped shape recording artists' visions and expand their commercial reach.[17] We embrace AI as a tool to *support* human creativity, provided that it is not used to *supplant* human creativity.

Artificial Intelligence and Copyright, available at https://www.regulations.gov/comment/COLC-2023-0006-8833 and https://www.regulations.gov/comment/COLC-2023-0006-8833 ("Copyright Office Comments").

[11] *See* https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/11/01/remarks-by-vice-president-harris-on-the-future-of-artificial-intelligence-london-united-kingdom/.

[12] U.N. Universal Declaration of Human Rights, art. 27, § 2 ("Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author"), available at https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[13] U.S. Const. art. 1, § 8, cl. 8 ("To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries").

[14] Title 17, United States Code.

[15] *See, e.g.,* the U.N. Universal Declaration of Human Rights, art. 12 ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.").

[16] AI RMF, p. 16, ("Training data may also be subject to copyright and should follow applicable intellectual property rights laws.") and p. 24 (includes in the govern function a recommendation that "[p]olicies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights"), available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[17] For example, a foreign artist signed to one of our member companies used a generative AI system to train on recordings of his vocals – allowing him to simultaneously release his single in six languages – in his own voice – on

However, we have already experienced harm from the unethical development and deployment of AI systems that unfairly exploit artists' and our members' expression, creative contributions, names, images, voices, and likenesses without their consent and without compensation. For example, several music publishers recently sued Anthropic for systematic and widespread infringement of their copyrighted song lyrics by unlawfully copying and disseminating those lyrics in connection with Anthropic's AI development and deployment.[18] In addition, beginning in 2023, there has been an explosion of unauthorized AI vocal clones of recording artists, and unauthorized AI vocal clone "cover" recordings.[19] This harms the artists whose voices are being cloned and it infringes the rights of those that own the musical composition and the sound recording in each underlying track.[20] Others in the content sector have brought a host of lawsuits against AI companies, including claims against Meta, Google, OpenAI, Microsoft, Stability AI, and Midjourney, among others.[21] These infringements have devastating consequences on creators and rightsholders, resulting in reputational and economic harm.

Another harm associated with AI technology is that machine-generated material can be produced at a speed and scale that creates the very real potential for that material to overrun the marketplace, crowd out human-created work, and generally devalue works created by

---

the same day. In that example, the ethically trained tool enhanced and extended the artist's creative intent – with his consent – enabling him to reach new markets and fans. *See also* Jeff Benjamin, *HYBE's 'New" K-Pop Artist MIDNATT Is Using AI Technology for a Remarkably Human Purpose*, Billboard (May 17, 2023), https://www.billboard.com/music/pop/artificial-technology-kpop-artist-midnatt-hybe-interview-1235329459/.

[18] Concord Music Group Inc. v. Anthropic PBC, (M.D. Tenn. Oct. 18, 2023). We have also witnessed a disturbing practice of willfully disaggregating the creation of datasets containing copyrighted works for AI training, often by entities that claim to be non-profit or research focused, and the actual training of AI models, often by for-profit commercial entities. *See* Oct. 30, 2023 Copyright Office Comments, p. 12 for more details.

[19] Collectively, just five of the popular sites to generate unauthorized AI vocal covers received nearly 100 million visits in 2023. The music industry has sent takedown notices for tens of thousands of such unauthorized recordings that infringe the rights of recording artists and rightsholders. *See also, e.g.*, Dani Di Placido, *Thanks to AI, Fake Kanye and Drake Songs are Going Viral on TikTok*, Forbes (Apr. 24, 2023, 10:07 AM), https://www.forbes.com/sites/danidiplacido/2023/04/24/ai-generated-songs-that-sound-like-kanye-and-drake-are-going-viral-on-tiktok/?sh=1f9bfcf13531.

[20] Several artists have spoken out against such vocal cloning and other unauthorized uses of generative AI. *See, e.g.*, Julia Gray, *All the Artists Who Have Spoken Out Against AI Music This Year,* The Messenger (Nov. 14, 2023 10:49 AM, https://themessenger.com/entertainment/artists-against-ai-music-quotes-bad-bunny. Also, as noted in section 2.2 of our comments, the proliferation of such tools to clone a person's name, image, voice, or likeness without their consent extends far beyond the music industry. These tools can be used by anyone to create voice, image, or likeness of any person, and spread deceptions that sound or look eerily realistic. Such AI-generated material made without the person's consent is not the public interest and harms our society. *See e.g.,* Derrick Bryson Taylor, *Tom Hanks Warns of Dental Ad Using A.I. Version of Him,* New York Times, Oct. 2, 2023, https://www.nytimes.com/2023/10/02/technology/tom-hanks-ai-dental-video.html. *See also* fn 45; OSTP Comments, p. 8-9.

[21] *See, e.g.*, Ivan Moreno, *Copyright Cases to Watch in 2024,* Law360 (Jan. 1, 2024), https://www.law360.com/articles/1777848/copyright-cases-to-watch-in-2024.

human beings.[22] This can divert the flow of royalties and engagement away from human creators,[23] and devalues human artistry.[24]

Various levels of government have warned of these harms and called for action to mitigate them. For example, the White House President's Council of Advisors on Science and Technology (PCAST) cautioned that generative AI systems can "undermine intellectual property rights."[25] The FTC warned that such unauthorized vocal cloning could "jeopardize an artist's reputation and ability to earn income."[26] The Government Accountability Office noted economic issues arising from generative AI systems trained on copyrighted, proprietary, or sensitive data, without the owner's or subject's knowledge.[27] Congress has held various hearings on these issues noting these concerns,[28] and introduced bills to reduce some of these harms.[29]

NIST's focus in response to the Executive Order should be to promote guidelines, standards, and best practices to reduce these harms (among others).[30] Moreover, in light of the impact generative AI has on the music community, all of the relevant stakeholders, including music creators and rightsholders, should be at the table for the development of such guidelines,

---

[22] *See, e.g.*, Daniel Tencer, *AI Music App Boomy Has Created 14.4M Tracks to Date. Spotify Just Deleted a Bunch of Its Uploads After Detecting 'Stream Manipulation,'* Music Business Worldwide (May 3, 2023), https://www.musicbusinessworldwide.com/ai-music-app-boomy-spotify-stream-manipulation/ ("According to Boomy's website, since the AI startup was founded in the U.S. in 2019, its users have created a whopping 14.4 million songs, which, the firm boasts, accounts for "around 13.78% of the world's recorded music.").

[23] AI-generated music can also be used as a tool for fraud and to illegally siphon royalties away from artists and rightsholders. We are seeing uploads of AI-generated tracks followed by bots that are used to create "fake listens" of those tracks through the practice of so-called "stream manipulation."

[24] We also note this can ultimately harm the progress of generative AI, as generative AI needs quality human made materials for its training. *See* Sina Alemohammad et. Al., *Self-Consuming Generative Models go MAD,* arxiv.org, July 4, 2023, https://arxiv.org/pdf/2307.01850.pdf.

[25] *PCAST Working Group on Generative AI Invites Public Input*, May 13, 2023, available at https://www.whitehouse.gov/pcast/briefing-room/2023/05/13/pcast-working-group-on-generative-ai-invites-public-input/#:~:text=The%20President's%20Council%20of%20Advisors,equitably%2C%20responsibly%2C%20and%20safely%20as.

[26] *Preventing the Harms of AI-enabled Vocal Cloning*, FTC's Office of Technology and Division of Marketing Practices, Nov. 16, 2023, available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/preventing-harms-ai-enabled-voice-cloning.

[27] *See* "Science and Tech Spotlight: Generative AI," Jun. 13, 2013, GAO-23-106782, available at https://www.gao.gov/products/gao-23-106782.

[28] *See, e.g.,* Senate Judiciary Subcommittee on Privacy, Technology and the Law Hearing titled *Oversight of A.I.: Rules for Artificial Intelligence*, May 16, 2023, https://www.c-span.org/video/?528117-1/openai-ceo-testifies-artificial-intelligence ("May 16, 2023 Hearing"); House Judiciary IP Subcommittee hearing titled *Artificial Intelligence and Intellectual Property: Part I: Interoperability of AI and Copyright Law*, May 17, 2023, https://youtu.be/Mm1NQ_Kqumw ("May 17, 2023 Hearing").

[29] *See, e.g.,* No Artificial Intelligence Fake Replicas and Unauthorized Duplications (No AI FRAUD) Act, H.R. 6943, AI Foundation Model Transparency Act of 2023, H.R. 6881, and AI Labeling Act of 2023, H.R. 6466.

[30] Because of the rapid pace of generative AI development and its potential to be used for malicious purposes, NIST should have a process for ongoing research and best practices improvement to keep pace with such development.

standards, and best practices. Such an important undertaking should not be left solely to the AI developers.

Guidelines, Standards, and Best Practices. In light of the foregoing concerns, we recommend that NIST adopt the following guidelines, standards, and best practices concerning generative AI.

Licensing and Clearances. AI developers should first obtain appropriate licenses and authorizations in connection with any copyrighted materials they desire to copy and ingest for AI development purposes before engaging in such copying or ingestion, and AI developers must refrain from engaging in any such copying or ingestion unless and until they have received such licenses and authorizations.[31] In addition, AI developers and deployers should implement appropriate safeguards to respect the rights of third parties, including procedures to determine whether their use of any ingested materials (whether in the AI model development, deployment, or output) implicate a person's copyrights, a person's rights to the use of their name, image, voice, and likeness, or a person's right of privacy. If the ingested materials or their proposed use implicate any such rights, it should be clear that AI developers must first obtain appropriate licenses, consents, and authorizations from the applicable rightsholders before ingesting or using such materials.[32]

This is true for anyone in the AI "supply chain" that is exploiting any of these third-party rights.[33] For example, where AI developers incorporate models from third parties, the AI developer must either obtain licenses directly from all affected copyright owners or obtain a sublicense from the party that created the model, after using due diligence to confirm that the party that created the model has all rights necessary to grant such a sublicense.

---

[31] This is consistent with the general approach in the Copyright Act, which establishes an opt-in, permissions-based regime with limited exceptions or limitations. 17 USC § 101 et seq. *See also* comments of Sam Altman, CEO of Open AI, at the May 16, 2023 Hearing, starting at 1:07:44 ("creators deserve control over how their creations are used and what happens beyond the point of them releasing it into the world"); comments of Ed Newton-Rex in *Why I just Resigned from my Job in Generative AI,* Music Business Worldwide, Nov. 15, 2023, https://www.musicbusinessworldwide.com/why-just-resigned-from-my-job-generative-ai/# ("[T]raining generative AI models in this way is, to me, wrong. Companies worth billions of dollars are, without permission, training generative AI models on creators' works, which are then being used to create new content that in many cases can compete with the original works. I don't see how this can be acceptable in a society that has set up the economics of the creative arts such that creators rely on copyright.").

[32] As noted in the Copyright Office Comments, the music industry has successfully licensed its large catalog of works for new business models for several years, and the latest new business model - generative AI - should not be treated differently.

[33] Requiring all parties in the supply chain to have the necessary licenses/permissions is nothing novel. Newspapers (and other media businesses), for example, deal with this all the time. If a newspaper wants to publish a photograph that it acquires from a third party (e.g., a newswire, a stock photography company), it must ensure that its source obtained the photograph legally and that it is permitted to sublicense downstream users. Movie studios have teams of people that clear third-party works for inclusion in motion pictures and television shows. And our members have clearance departments that clear rights to third-party samples, artwork, and so forth. AI developers should not be treated any differently.

Recordkeeping and Transparency. AI developers and AI deployers should be required to collect, maintain, and disclose (as appropriate) proper records concerning the entire AI development and deployment lifecycle.[34] Proper recordkeeping should include complete documentation about:

(i) what materials were ingested to develop the AI system (or to fine tune or adapt a pre-trained AI system) and in what manner, [35]
(ii) the provenance of such materials, including whether any licenses or authorizations were sought or obtained to authorize such use and copies of those licenses or authorizations,
(iii) the articulated rationale for selecting and using the materials ingested for the AI system's development,
(iv) the articulated purpose of the AI model itself and its intended outputs,
(v) the AI system's overall functioning,
(vi) the individual or organization responsible for the AI system (including who is responsible for ingesting the materials, who is responsible for any foundational AI model, who is responsible for any fine tuning of the AI model, who is deploying the AI system, etc.),
(vii) risk assessments concerning the potential misuse and abuse of such a model,
(viii) what parameters and processes were used, and what decisions were made, during the AI system development and deployment, and
(ix) such other information relevant to explain, interpret, and understand the decision-making process used within the AI system, and its resulting output.

Such recordkeeping should occur at various times within the AI development and deployment process, including when an AI system is developed, when it is fine-tuned or adapted for a particular purpose or use case, when the system is deployed, and when problems with the system are uncovered, analyzed, and addressed.[36] Consistent with this principle, AI developers and deployers who use third-party training datasets or pre-trained models should also obtain and maintain adequate records from upstream sources concerning those training sets or models. In addition, these records should be kept throughout the AI system's development and deployment lifecycle, and for a period of at least seven years following its discontinuance.

With regard to transparency, AI developers and deployers should disclose to the public and regulators the purpose of the AI system and its overall functionality, who is the individual or entity responsible for the AI system and their location and contact information, the provenance of the materials ingested during the AI system's development, and basic information to provide

[34] Similarly, those who collect and curate copyrighted works for ingestion by AI tools should also be required to collect and retain records regarding the materials they have collected for AI ingestion, and to whom they have licensed or provided access to such materials and for what purpose.
[35] This information should be granular enough that a rights owner can review the records and determine if their works have been ingested. For recorded music, that means that AI developers would have to track fields including, but not necessarily limited to, track title, artist name, songwriter name, ISRC, ISWC P-line, and C-line.
[36] Goodman, Ellen et al., "AI Audit-Washing and Accountability," G.M.F., Nov. 15, 2022, p. 18, available at https://www.gmfus.org/news/ai-audit-washing-and-accountability.

algorithmic transparency.[37] This information should be disclosed to regulators, interested parties, and the general public at a level of specificity necessary to address their legitimate concerns relating to the development, training, and operation of AI systems. AI developers and deployers should also make more detailed records and audits of the AI system available to third parties who have a good faith claim that their rights have been violated in connection with the AI system's development or deployment.

Because the development of an AI system is often not in the public eye, requiring such records to be maintained, audited periodically, and disclosed where applicable, will help improve accountability, and ultimately the safety and security of the AI system. In fact, a variety of companies and groups within the tech sector seem to regard such recordkeeping and transparency as both broadly beneficial and achievable.[38]

Audits and Assessments. The AI systems, and their records, should be audited periodically throughout the AI development and deployment lifecycle.[39] These audits should include, among other things, checks on the provenance of data sources (including checks for intellectual property ownership and related issues and whether licenses and clearances have been properly obtained), AI validation checks that include checks for information leakage (which could result in a security breach, personal data breach, or infringement of copyright), checks on transparency and human oversight during deployment, checks on the impact and survivability of any labeling, and checks on long term consequences of AI deployment, including its social impact and model drift.[40] AI audits should occur not only prior to releasing an AI system to the public, but also before the training of an AI system commences and any time the system is updated in any material way.[41]

AI developers (and AI deployers, as applicable) should also identify and document risk assessments and their plans to mitigate those risks in the development and deployment of their AI models. Those risk assessments should include intellectual property infringement risks including violations of a person's rights of name, voice, image, and likeness and right of privacy,

---

[37] This is consistent with the *White House Blueprint for an AI Bill of Rights*, The White House, https://www.whitehouse.gov/ostp/ai-bill-of-rights/, and congressional calls for disclosure requirements for AI systems, such as those expressed at the May 16, 2023 Hearing and the May 17, 2023 Hearing.

[38] *See, e.g.,* Hugging Face Initial Comments to the Copyright Office in the Matter of Artificial Intelligence and Copyright at 2, 12 ("Hugging Face Initial Comments"); Comments Filed by Google in Response to National Telecommunications and Information Administration AI Accountability Policy Request for Comment at 23, ("AI developers can support accountability by retaining detailed documentation of datasets and models").

[39] *See* Written Testimony of Professor Gary Marcus before the Senate Judiciary Subcommittee on Privacy, Technology and the Law titled *Oversight of A.I.: Rules for Artificial Intelligence,* May 16, 2023, available at https://www.judiciary.senate.gov/imo/media/doc/2023-05-16%20-%20Testimony%20-%20Marcus.pdf ("Marcus Testimony"). *See also* the comments from researchers from the Stanford Center for Research on Foundation Models, part of the Stanford Institute for Human Centered Artificial Intelligence and Princeton University's Center for Information Technology Policy, in response to NTIA's request for comments on AI Accountability Policy, available at https://hai.stanford.edu/sites/default/files/2023-06/Response-to-Request.pdf.

[40] *See* Van Otterloo, "A checklist for auditing AI systems," ICT Institute, Dec. 18, 2022, available at https://ictinstitute.nl/a-checklist-for-auditing-ai-systems/.

[41] *See* Marcus Testimony.

as well as broader risk assessments concerning the misuse or abuse of an AI model. These risk assessments would benefit from red teaming to evaluate whether the AI training material and/or the AI system's output implicate any of the risks listed above.[42]

Economic Implications. The activities described above, including recordkeeping, transparency, labeling, auditing, and assessments, are necessary for, and simply the cost of, developing and deploying safe, secure, accountable, and trustworthy AI systems. Although the cost of such activities should be fairly trivial in the broader context of full AI development and deployment costs,[43] even if that were not the case, the cost (or exaggerated claims about the cost) should not be a reason not to require AI developers to engage in such activities. Moreover, the economic implications of such activities must be weighed against the significant economic and reputational harms to a much larger swath of third parties if such activities were not adopted.

The sort of recordkeeping proposed above should be easily automated, especially if the various entities involved in the AI supply chain ensure that the metadata that accompanies legitimately sourced music is maintained along with the music files themselves. Indeed, there are already companies in the marketplace that provide services to help with and automate such recordkeeping.[44] For example, an AI dataset or model that includes sound recording ISRCs or musical work ISWCs should be able to easily identify the key data fields associated with each such sound recording or musical work, as applicable and use that data to automatically populate a recordkeeping template.

Similarly, in terms of risk assessment, AI developers could use audio fingerprinting technology and melody matching technology, which are relatively inexpensive, to scan the sound recordings in a proposed dataset to be used for AI training or finetuning,[45] detect their titles and other relevant data fields, and use that information to assess the risk of using those sound recordings for AI development or deployment purposes.[46]

---

[42] While providing guardrails on the output of an AI system may mitigate some of these risks, they do not eliminate or discharge the harm caused by copying and ingesting infringing materials without authorization for AI development. In fact, such guardrails may well mask those very harms.

[43] *See e.g.,* Hugging Face Initial Comments at p. 12 ("The cost of proper documentation is marginal when done along with the initial research, but can be significant when done a posteriori. We believe the broad benefits are substantial, both from a copyright perspective and aligning with broad recommendations about responsible AI development and public interest.").

[44] *See, e.g.*, Marius Schlegal & Kai-Uwe Sattler, *Management of Machine Learning Lifecycle Artifacts: A Survey*, arXiv, Oct. 21, 2022, available at https://arxiv.org/pdf/2210.11831.pdf (reviews a representative selection of more than 60 systems and platforms).

[45] Similarly, AI deployers could assess and reduce the risk of infringement in an economical manner by assessing the risk of user prompts using automated content recognition, melody matching, and metadata matching technologies.

[46] Neither the volume of the data nor the allegedly competitively sensitive nature of the works used for ingestion are reasons to avoid recordkeeping and disclosure obligations in appropriate circumstances. Concerns about competitive sensitivity can be addressed by limiting access to sensitive information to stakeholders with a legitimate need to know (e.g., regulators, rights owners).

2. Reducing the Risk of Synthetic Content

As noted previously, due to the easy access the public has to powerful generative AI tools, anyone can use such tools to generate fake or malicious content that robs music professionals of the economic potential for their creative expression,[47] defrauds fans into believing artists and songwriters they love created music that they did not create, and harms society more generally with scams, cybercrime, deep-fake porn, and risks to national security.[48] Reducing the risks of such synthetic content involves a multi-disciplinary and iterative approach.

Labeling Synthetic Content and Resilience of Techniques for Doing So. Content purely generated with AI should be appropriately labeled. We presume there are no insurmountable barriers to such labeling as several AI companies have voluntarily committed to provide such identification.[49] However, we have concerns with the use of bespoke watermarking technology by each individual AI company. To help downstream providers make such watermarks readable and accessible to the public, it would useful if there could be some standardization or consistency for watermarking, or the payload that is used for watermarking, for each media type. Having downstream providers make such watermarks readable and accessible to the public is essential to fulfill the goal of informing consumers and others that the content is synthetic. We also have concerns with the fragility of the watermarks that may be used. We recommend that they be tested to confirm they survive standard digital file manipulations,[50]

---

[47] *See* fn 20. *See also* Lionel Laurent, *AI Music Brings the Sound of Scammers to Spotify,* Washington Post, May 11, 2023, https://www.washingtonpost.com/business/2023/05/11/m/3c7f3be4-efb3-11ed-b67d-a219ec5dfd30_story.html.

[48] *See e.g., Attack Vectors 2024: Protecting Against What's Next in Deepfake Fraud,* PYMTS, Jan. 9, 2024, https://www.pymnts.com/fraud-prevention/2024/attack-vectors-2024-protecting-against-whats-next-in-deepfake-fraud/; Luc Cohen, *AI advances risk of facilitating cyber crime, top US officials say,* Reuters, Jan. 9, 2024, https://www.reuters.com/technology/cybersecurity/ai-advances-risk-facilitating-cyber-crime-top-us-officials-say-2024-01-09/; Skyler Harris and Artimis Moshtaghian, *High schooler calls for AI regulations after manipulated pornographic images of her and others shared online,* CNN, Nov. 4, 2023, https://www.cnn.com/2023/11/04/us/new-jersey-high-school-deepfake-porn/index.html; Hannah Murphy, *The rising threat to democracy of AI-powered disinformation*, Financial Times, Jan. 11, 2024, https://www.ft.com/content/16f23c01-fa51-408e-acf5-0d30a5a1ebf2; Rebecca Klar, *AI 'wild west' raises national security concerns,* The Hill, Mar. 8, 2023, https://thehill.com/policy/technology/3888433-ai-wild-west-raises-national-security-concerns/; Mohamed R. Shoaib et al, *Deepfakes, Misinformation and Disinformation in the Era of Frontier AI, Generative AI, and Large Language Models,* arxiv.org, Nov. 29, 2023, https://arxiv.org/pdf/2311.17394.pdf ("Shoaib Deepfakes Paper").

[49] *See, e.g., Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI,* The White House, July 21, 2023; *Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI,* The White House, Sept. 12, 2023.

[50] *See, e.g.*, Yongbaek Cho et al, *Attributable Watermarking of Speech Generative Models,* arXiv.org, Mar. 15, 2022, https://arxiv.org/pdf/2202.08900.pdf; Xuandong Zhao, *Invisible Image Watermarks are Provably Removable Using Generative AI*, arXiv, Aug. 6, 2023, https://arxiv.org/pdf/2306.01953.pdf; *see also* Kate Knibbs, *Researchers Tested AI Watermarks – and Broke All of Them*, Wired (Oct. 3, 2023), https://www.wired.com/story/artificial-intelligence-watermarking-issues/; Lijun Zhang, *Robust Image Watermarking Using Stable Diffusion,* arXiv.org, Jan. 8, 2024, https://arxiv.org/pdf/2401.04247.pdf.

and updated as necessary to survive typical and emerging digital file manipulation techniques. We also note that the audio watermarking space keeps evolving, with a recent article suggesting a watermarking technique that encodes up to 32 bits of watermark within a 1 second audio snippet.[51]

Detecting Synthetic Content. Various tools exist and/or are in the process of development to detect deep-fake synthetic content.[52] These include machine learning algorithms that analyze video frames for signs of manipulation at the pixel level, and those that analyze audio for irregularities in vocal or singing patterns, background noise, or other irregularities or artifacts in non-vocal audio, including music.[53] Many of these tools also rely on other indicators, such as metadata associated with the digital content at issue. However, as commentators have noted, the challenge with these tools "lies in the fact that as the detection algorithms become more sophisticated, so too do the methods for creating deepfakes, leading to an ongoing arms race".[54]

Authenticating Content and Tracking its Provenance. Various methods have been proposed for authenticating content and tracking its provenance. These include the use of digital watermarking upon creation of the content, authentication protocols such as those from the Coalition of Content Provenance and Authentication (C2PA), use of blockchain technology to track the content, and the use of biometric authentication methods.[55] Similar to detection technologies, however, authentication and provenance tracking also involves an ongoing arms race to keep up with deep fake developments.

Other Approaches. In addition to the methods noted above to deter or detect synthetic content, and the need for the constant evolution of those methods, NIST should consider recommending a multidisciplinary and iterative approach to address this problem. Such an approach could include multistakeholder collaboration to address existing and emerging threats, and a joint response framework among internet companies (digital service providers, social media platforms, search engines, etc.) to address known deep fakes.[56] With respect to audio, researchers have recently suggested a system that would "make an active effort to watermark the generated speech in a way that aids detection by another machine," based on

[51] Guangyu Chen et al, *WavMark: Watermarking for the Audio Generation,* arXiv.org, Jan. 7, 2024, https://arxiv.org/pdf/2308.12770.pdf.
[52] *See, e.g.,* https://www.pindrop.com/deepfake; https://realitydefender.com/; https://www.resemble.ai/detect/; https://thesentinel.ai/; https://weverify.eu/about-us/overview/#1560343088338-24c0bae8-7ae8.
[53] *See, e.g.,* Shoaib Deepfakes Paper. There are also detection tools for vocal audio that measure the physical aspects of a person's voice to detect if the test audio stream is authentic or synthetic, and tools to detect synthetic vocals when singing. *See, e.g.,* https://virvii.ai/; ttps://www.matchtune.com/covernet-music-copyright-infringement-detection.
[54] Shoaib Deepfakes Paper. *See also* Pavel Korshunov et al, *Vulnerability of Automatic Identity Recognition to Audio-Visual Deepfakes,* arXiv.org, Nov. 29, 2023, https://arxiv.org/pdf/2311.17655.pdf.
[55] *Id.*; *see also* https://c2pa.org/.
[56] *Id.*

"collaborative training between a generative synthesis model and a watermarking detector."[57] Such approaches should be explored further.

3. Advancing Responsible Global Technical Standards for AI Development

AI Nomenclature and Methodology. We urge NIST to push back against attempts by others to anthropomorphize the AI development and deployment process and make it sound as if AI systems are "learning" information from input works or "creating" content the way that humans do. As one commenter noted, the "more we ascribe independence and autonomy to technology that's actually been designed and directed by specific people, the easier we make it for those people to shirk responsibility for its impacts and errors."[58] We should not allow such language to give cover to AI developers for their failure to fully understand or explain the outputs from their AI systems.[59] Instead, NIST should follow the approach taken in the G7 Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System and Code of Conduct for Organizations Developing AI systems, which clearly call on the organizations developing or deploying these systems to take the actions set forth in those documents. In addition, we urge NIST to intentionally use nomenclature in all of its papers, recommendations, best practices, and the like that ascribes agency to the humans behind the AI, not to the AI itself.

Follow G7 Principles and Best Practices. We urge NIST to promote and follow the principles set forth in the G7 Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System and Code of Conduct for Organizations Developing AI systems, and the best practices noted in section 1 above. Further, in order to protect the human rights of songwriters, sound recording artists, and other authors of human creative works, we urge NIST to reject calls for text and data mining exceptions.[60]

Include Creators and Rightsholders in the Standards Development Process. As noted previously, creators and rightsholders, including our members and those they represent, should have a seat at the table in the AI standards development process. NIST should reach out, and encourage other governments and standards bodies to reach out, to organizations in the creative sector, such as their trade associations in various countries to ensure their views are heard.

---

[57] Lauri Juvela and Xin Wang, *Collaborative Watermarking for Adversarial Speech Synthesis,* arXiv.org, Jan. 2, 2024, https://arxiv.org/pdf/2309.15224.pdf.

[58] Scott Rosenberg, *AI's colossal puppet show,* Axios, Dec. 20, 2023, https://www.axios.com/2023/12/20/ai-puppet-show-robots-autonomy.

[59] *Id.*

[60] Recently, Prof. Eleonora Rosati described why the text and data mining exceptions in Japan and Singapore should not allow unrestricted use of copyrighted content for the creating of training sets and AI training under the three-step test. *See* Eleonora Rosati, *No Step-Free Copyright Exceptions: The Role of the Three-step in Defining Permitted Uses of Protected content (including TDM for AI-Training Purposes)*, Nov. 10, 2023, SSRN: https://ssrn.com/abstract=4629528 or http://dx.doi.org/10.2139/ssrn.4629528.

* * *

We thank NIST for the opportunity to respond to this RFI. Please let us know if you have any questions or if we can provide any additional input. We look forward to continuing this conversation with NIST and other policy makers as AI technology and its impact on the marketplace and society evolves.

Respectfully submitted on behalf of A2IM, NMPA, and RIAA,

/Victoria Sheckler/
Victoria Sheckler
SVP, Deputy General Counsel
Recording Industry Association of America