

Nonprofits and AI: Managing Legal and Other Risks

*by Holly E. Peterson, Esq., Counsel
Tenenbaum Law Group PLLC*

Generative artificial intelligence (AI) is ubiquitous. Even those most skeptical of AI almost certainly use AI as matter of routine, whether through the spell-check feature in Microsoft Word, the auto-correct feature in text messages, the auto-complete feature in various applications, web searches, closed-captioning, digital traffic maps, smart home devices, suggested responses on Gmail, Siri, and so forth. At this point in time, it is not realistic to imagine a business where AI is not used in some form. Even so, nonprofit organizations should carefully weigh the benefits of AI against legal and reputational risks. For example, a nonprofit may wish to authorize the use of AI to capture committee or working group notes, but, might there ever be times when such authorization is imprudent, for example, if a committee or working group is discussing sensitive, confidential, or proprietary information? Consider another example where a nonprofit uses AI to assist in the peer review of a journal article. This could be efficient and highly valuable, but it also could prompt legal, reputational, or scholarly concerns.

As technology evolves, AI will become more and more intertwined into the fabric of nonprofit operations. Nonprofit leaders should thoughtfully consider the promise and perils of AI with respect to their organization's specific needs and should thoughtfully craft policy and practice that is tailored to the nonprofit's specific needs, all the while managing legal and reputational risks and aligning policy with accepted practices, industry standards, and strategic aspirations. This article outlines legal, reputational, and other risks related to AI and outlines some strategies for managing those risks.

1. Primary Risk Areas

While the promise of AI presents transformative opportunities, the use of generative AI presents legal and other risks that must (and can) be managed. Primary risk areas include intellectual property¹ ownership, use, and infringement, privacy and data security, discrimination, and tort liability. These risks are borne from a complicated web of evolving federal, state, and international laws related to privacy and data security and, to a lesser extent, to AI itself, that in many ways intersect but that all have various nuances. In addition to legal risks, AI also may present reputational risks. While the potential risks are significant, appropriate risk mitigation measures can reduce both legal exposure and reputational risk.

A. Who owns the copyright to AI-generated content?

¹ While "intellectual property" includes copyrights, trademarks, patents, and trade secrets, for the purpose of this article, it is primarily referring to copyright.

The U.S. Copyright Office will only register an original work of authorship that has been “created by a human being.”² The Office’s Compendium of Copyright Office Practice clarifies that “the Office will not register works produced by a machine or mere mechanical process that operates randomly or automatically without any creative input or intervention from a human author.”³ To evaluate ownership claims, the Office will look at “whether the ‘work’ is basically one of human authorship, with the computer [or other device] merely being an assisting instrument, or whether the traditional elements of authorship in the work (literary, artistic, or musical expression or elements of selection, arrangement, etc.) were actually conceived and executed not by man but by a machine.”⁴ The U.S. Copyright Office reaffirmed this position, most recently in an August 30, 2023 call for comments published in the Federal Register, but, in so doing, acknowledged the inherent challenge in discerning between AI-generated content and human-generated content, especially when a new work had both human and artificial imprints. As it reflected, “Although we believe the law is clear that copyright protection in the United States is limited to works of human authorship, questions remain about where and how to draw the line between human creation and AI-generated content.”⁵

AI ownership is a novel and rapidly evolving area of law.⁶ Based on existing law, nonprofit organizations should assume that they have no intellectual property rights in and with respect to AI-generated content. As a matter of course, nonprofit entities should require human authors to substantially and materially contribute to any nonprofit work product.⁷ Nonprofits should revise existing author and speaker agreements (both for volunteers and paid contributors) to require a written attestation from employees, contractors, and volunteer authors and speakers representing and warranting that (i) any submitted content has been revised substantially such that the author/creator has all necessary rights to assign or license the work to the nonprofit and (ii) the submitted content does not infringe the intellectual property rights of any third party. As discussed later in this article, that same attestation should also address defamation, privacy, and other third-party rights. At least for paid contributors, the author/creator should indemnify the nonprofit for any breach of these representations and warranties.

B. What third-party intellectual property rights exist that could be leveraged into an actionable claim against a nonprofit for the improper use of AI?

² U.S. Copyright Office, Compendium of the U.S. Copyright Office Practices at 7 (3d ed. Jan. 28, 2021).

³ *Id.* at 21-22.

⁴ *Id.*

⁵ U.S. Copyright Office, Artificial Intelligence and Copyright, Fed. Reg. Vol. 80, 59943 (Aug. 30, 2023).

⁶ In March 2023, the U.S. Copyright Office launched an initiative to examine copyright law and policy in relation to AI. It issued its first report on Digital Replicas on July 31, 2024. For more information, see <https://www.copyright.gov/ai/> (last visited Aug. 5, 2024).

⁷ U.S. Copyright Office, Artificial Intelligence and Copyright, Fed. Reg. Vol. 80, 59943 (Aug. 30, 2023) (contributions must be more than *de minimis*).

Under U.S. copyright law, a copyright holder has the sole and exclusive rights to create derivative works from the underlying copyrighted work, unless the author assigns or licenses that right to a third party. “[A] ‘derivative work’ is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted.”⁸

Assume that an author/contributor submits an original work that relies, in part, on AI-generated content and that the nonprofit publishes the work on its website and distributes the work to its membership. Assume also that the AI-generated content that is embedded in the submitted work infringes someone else’s copyright. It is possible, in this circumstance, that the third party whose copyright was infringed may have actionable claims against the author and against the nonprofit that published and redistributed the work. Ultimately, an infringement claim will hinge on the facts, focusing on the extent of the infringement, as well as an analysis of whether the appropriated content amounts to permissible use under the Fair Use Doctrine.

The factual analysis, though, is hardly simple. Even the U.S. Copyright Office is not certain how to distinguish new works from derivative works when AI is used in the development of a work. They have asked for public input on (1) “whether or when the use of copyrighted works to develop datasets for training AI models (in both generative and nongenerative systems) is infringing”; (2) “the proper scope of copyright protection for material created using generative AI”; and (3) how liability should be apportioned for AI generated content that infringes upon a copyright.⁹

As before, risk can be mitigated by requiring human authors to indemnify the nonprofit for works that infringe upon third-party intellectual property rights.¹⁰ Indemnity essentially transfers risk from the nonprofit to the submitting author, thus protecting the nonprofit from any liability that might arise from third-party intellectual property claims. That being said, for volunteer authors, it often can be difficult to get them to agree to such indemnification.

C. What are the legal risks of using AI with respect to privacy and data security?

Nonprofit organizations use of AI, while embedding great promise, also carries substantial risk, especially with respect to privacy and data security.¹¹ AI relies on inputted

⁸ U.S. Copyright Act, 17 U.S.C. §1101.

⁹ U.S. Copyright Office, Artificial Intelligence and Copyright, Fed. Reg. Vol. 80, 59943 (Aug. 30, 2023).

¹⁰ U.S. Copyright Office, Artificial Intelligence and Copyright, Fed. Reg. Vol. 80, 59943 (Aug. 30, 2023) (contributions must be more than *de minimis*).

¹¹ President Biden’s Executive Order, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Oct. 30, 2023). Note that this Executive Order merely directs federal agencies to develop policies

data to generate new data. It does not differentiate between public data and personally identifiable information (“PII”) or confidential information. Because PII is so heavily regulated by federal, state, and international law, nonprofits should not allow staff, contractors, volunteer contributors, or other agents to input PII into an AI application unless comprehensive compliance measures are implemented and enforced. For other reasons—namely to safeguard confidential, proprietary, sensitive, and/or attorney-client privileged information—nonprofits also should prohibit staff, contractors, volunteer contributors, and other agents from inputting confidential, proprietary, or sensitive information or privileged content of any sort into any AI application—even if the “sharing”/“learning” feature of the AI application is disengaged, as can be done with paid and enterprise versions of most of the leading AI platforms.

If it is not possible or practicable to segregate PII or other confidential information—for example, if a nonprofit uses targeted advertising to tailor member or donor experiences—the organization should implement additional risk mitigation measures to comply with federal, state, and international data privacy laws. While each of these laws contains various nuances, in general, these robust laws derive from a uniform set of principles that endeavor to protect PII from unauthorized disclosure by (1) requiring organizations to obtain informed consent prior to collecting and using PII, (2) requiring that organizations provide an opportunity for individuals to change their preferences at any time about whether and how their data will be used, and (3) requiring organizations to provide a mechanism for individuals to access personal data. A robust privacy and data security policy, coupled with aligned organizational practice, can help to mitigate liability for a data breach. Where a nonprofit relies more heavily on sensitive PII, we recommend engaging expert privacy counsel to (1) determine applicable data privacy laws, (2) review and classify all existing data that may be used by the AI application, (3) identify the purpose and use of the data in a clear and articulable way, (4) develop a compliance plan, and (5) monitor compliance over time and take appropriate action in the event of noncompliance.

D. What are the legal risks of using AI with respect to discrimination?

In an October 2023 Executive Order, President Biden acknowledged the perils of AI in perpetuating discrimination: “Artificial Intelligence systems deployed irresponsibly have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms.”¹² Indeed, because AI relies on pre-existing inputted data, it can inadvertently replicate and perpetuate bias and discrimination. We have seen this play out most prominently in the human resources context, where AI resume review has the potential to introduce unlawful bias into the hiring process, exposing nonprofit and for-profit entities to legal liability under Title VII of the federal Civil Rights Act,

and procedures regarding the use of AI and does not apply to nonprofit organizations, but it does provide an excellent overview of some of the benefits and perils of AI.

¹² President Biden’s Executive Order, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Oct. 30, 2023).

state employment laws, and other federal, state, and local laws. Here, especially, it is critical for human reviewers to analyze and test for bias and/or discrimination.

While discrimination only creates legal exposure in certain contexts (*e.g.*, employment), algorithmic bias may have other adverse implications for nonprofit entities as well. Imagine, for example, that a nonprofit inputs 50 years of journal articles into a generative platform that conducts AI “peer reviews” of scholarly works. The peer review function draws from past scholarship to generate feedback on new works. Quite possibly, the generative feedback could rely on outdated nomenclature or debunked data in producing reviewer feedback that may be offensive, at best, or replicate biased or discriminatory scholarship, at worst. Whether or not that undesired result materializes, it is almost assured that use of an AI application of this sort will privilege existing content over novel theories, which could result in stagnation and stale scholarship, among other potential adverse consequences.

To best guard against this undesirable outcome, humans should always review AI processes and outputs for bias and/or discrimination and should record efforts to test for bias in meeting minutes (*e.g.*, documentation of a hiring process) or submit an attestation as an accompaniment to submissions fixed in any tangible medium (*e.g.*, written works, artistic works, videos, recordings, etc.).

E. What are the legal risks of using AI with respect to tort liability, scholarly reputation, and academic/professional integrity?

AI-generated content is not always accurate, potentially bearing on the reputation of a scholar, a scholarly publication, or a nonprofit publisher. To the extent that a statement of fact is not only false, but also adversely bears on a person’s reputation, the publication of the false statement could expose an author or publisher to liability for defamation. Again, sufficient human vetting is the best risk mitigation strategy to capture and correct factual inaccuracies. In addition, nonprofits should consider requiring that authors affix a conspicuous disclaimer to any submissions incorporating AI-generated content signaling that “the content was produced with the assistance of artificial intelligence” and that “the author/creator(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.” Disclaimers of this sort likely also will satisfy the ethical requirements embedded in some international AI laws.

2. Policy Development and Insurance Coverage

Nonprofit entities should develop and implement written AI usage policies, informed by the considerations outlined in this article as well as input from stakeholders familiar with various aspects of the nonprofit’s governance, management, and operations (*e.g.*, legal, technology, membership, finances, human resources, scholarly and educational departments, etc.). Some nonprofits have developed AI usage policies that cover everyone who uses AI for or on behalf of the organization (such as staff, contractors, and volunteer contributors), while others have created different policies for

different sets of users. Generally, and at a minimum, such policies should set forth a purpose, define material terms, scope coverage, describe permitted and prohibited uses of AI, require disclosures and disclaimers, and describe potential consequences of non-compliance. Because international data privacy and AI laws vary and continue to evolve, and because AI itself is rapidly evolving, nonprofit organizations should commit to revisiting the policy(ies) on a periodic basis to ensure that it/they remain(s) legally compliant, reflect(s) best practices and industry standards, and meet(s) the nonprofit's needs.

In addition, nonprofits should review their directors and officers liability and cyber insurance coverage, as well as their errors and omissions liability (sometimes called media liability) insurance coverage, to ensure that potential claims arising from the nonprofit's use of AI are covered to the greatest extent possible.

3. Conclusion

While the promise of AI presents transformative opportunities for nonprofits, the use of AI presents legal and other risks that must be managed and mitigated. Nonprofits should thoughtfully consider the benefits and perils of AI and craft thoughtful policies that appropriately circumscribe use in a legally compliant and ethical manner that, in all instances, aligns with the nonprofit's values, ethics, policies, and unique circumstances. Finally, be sure to revisit such policies on a regular basis, as this is, without question, a rapidly evolving area for every nonprofit organization.

* * * * *

For more information, contact Ms. Peterson at hpeterson@TenenbaumLegal.com.