ALM | LAW.COM

CORPORATE COUNSEL

# Are You Doing 'Deep Fake' Marketing? Consider Using a Scorecard

By Harry A. Valetk and Tal Dickstein

May 16, 2024

Generative artificial intelligence is dynamically revolutionizing the ways we develop new audio and video content for marketing initiatives and advertising campaigns. For those in-house counsel tasked with reviewing and approving these initiatives, understanding the potential legal risks, and assessing those risks efficiently, is increasingly becoming a business imperative. One of those new areas involves "deep fake" marketing.

By "deep fake," we refer to a combination of "deep learning" and replicating technology that leverages machine learning algorithms to create realistic—but "fake"—video and audio content of both actual or synthetic individuals. Two forms make up the bulk of the deep fake use cases: deep faces and deep voices. Deep faces replaces the faces of real people with virtual faces, or even creates an entirely synthetic face. Deep voices alters or mimics voices to make a real person appear to have said something they did not say. Thanks to the continuous evolution of AI-powered deep fake technology, we now have more sophisticated and convincing results that can be obtained in a matter of minutes for minimal cost.

AI's deep learning capabilities enable the computerized study and re-creation of human features that blur the line between fiction and reality. This evolutionary progress raises legal and ethical questions about the responsible use of AI when creating "deep fake" or synthetic marketing campaigns. When done lawfully and ethically, however, most marketing officers agree that synthetic marketing presents brands with untapped opportunities to lower campaign costs, produce better quality content, and engage with audiences in unprecedented ways through highly individualized storytelling experiences.

Credit: VectorMine/Adobe Stock

These experiences include, for example, interacting with a synthetic version of a living or deceased iconic figure. Fashion brands can showcase products on models with innumerable skin tones, heights, and body types presenting consumers with a more inclusive and relatable experience. In a global context, finding a local actor or model fluent in a language or dialect no longer needs to be a barrier to market entry. The same globally recognized artist can appear to speak hundreds of languages using deep voice overlays.

In this context, how can in-house counsel swiftly and competently assess legal risks for newly minted AI-driven campaigns? The answer lies in striking a balance of acceptable levels of legal risk, as defined within your organization, that conform with applicable industry standards, and guided by broader ethical considerations specific to your use case. With this in mind, assemble a scorecard with the following factors included to weigh the likelihood and severity associated with any deep fake marketing campaign.

### 1. Content-Driven AI Considerations

- **Visual vs. audio**. Is the content video or audio? While it is important to understand the copyright, right of publicity, intellectual property, licensing, and other legal restrictions for any content included in a marketing campaign, video content may pose additional legal risks.
- **Still vs. video**. Is the visual content a still or video? Does the still image qualify as artwork? Video presents more legal risk than a still image, as most marketing videos incorporate numerous individual images and personas, as well as audio. Understanding potentially applicable copyright protections, intellectual property, and other legal restrictions is important.
- **Music**. Does audio content qualify as music? Again, music likely presents additional legal risk since copyright protections may apply for both a particular sound recording as well as the underlying musical composition. Some lawyers argue that the biggest unresolved legal issue is whether artists, record labels, and publishers can claim infringement as AI learns from copyrighted works, even if the output bears little relation to the original compositions or lyrics.
- **Real people likeness or voices of actual persons**. Is content taken from the likeness of an actual living or deceased individual? Or is it the synthesized image and voice of a fictional character? Consent or other legal basis to use content may apply, including SAG-AFTRA union contract compliance obligations in the U.S., as well as endorsement rules.
- **Endorsements**. Marketing materials using AI actors/voices that include an endorsement present significant risk, even if a disclosure is provided such as "fictionalization using an AI-generated actor." It could be inherently and incurably deceptive to use an endorsement purporting to be spoken by a real human, about a personal experience that never happened, when, in fact, the person and experience do not exist. See the Federal Trade Commission's "Guides Concerning the Use of Endorsements and Testimonials in Advertising."
- **Kids**. Do any of the synthetic voice or visuals resemble or target children? Children are always afforded greater protections under the law, and will naturally present higher legal risk if prominently featured in a deep fake marketing campaign. In this regard, proceed with caution.
- **Outside the U.S.** Will the visual or audio content be used outside the U.S.? If so, consider potential local market restrictions beyond those set out above.

### 2. Legal and Litigation Landscape

- **U.S. Landscape**. The use of AI in any context remains new and quickly evolving under U.S. law. Many federal and state legislative proposals are being considered and enacted that would require the disclosure—and potentially limit the use—of AI in certain marketing contexts. It is important, therefore, to continually monitor the fast-moving legislative developments in this area.
- **Global Landscape**. If your content is being used outside the U.S., monitor legislative developments such as the European Union's Artificial Intelligence Act and other similar proposals.
- **Industry Landscape**. Numerous industries are also imposing specific guidance or other binding codes of conduct that may apply to the use of AI-driven marketing. One example is the SAG-AFTRA labor agreement covering the use of AI to digitally simulate the voice or likeness of a union member to create a new performance.
- **Contractual Landscape**. Risk allocation remains an unpredictable component in assessing legal risk. Advertisers, agencies, and others have yet to settle on industry standards for the use and deployment of AI-driven marketing. The same is true for insurers. Defining a clear company posture on risk tolerances in advance of a new AI-driven initiative will help your review proceed efficiently.
- **Litigation Landscape**. Courts are just now beginning to grapple with the broad use of AI in the marketplace, and have shown a reluctance to disturb the rights of individuals and organic human invention in the context of AI. For example, a district court recently found that works of art created by AI without any human input cannot be copyrighted under U.S. law. Only works with human authors can receive copyrights. Still, leveraging AI may infringe rights of human authors if the AI-generated material is substantially similar to an existing work that was used to train the AI platform.

### 3. Data Privacy and Security

- **Privacy and data protection**. The use of AI in any context remains new and unfamiliar; thus any AI-driven marketing campaign could provoke questions about the scope of consumer targeting, personalization, and tracking. Use of deep-fake technology to create and customize marketing content for different market segments could benefit from transparency to address privacy and data protection considerations. Above all, assess AI-driven marketing content for potential unethical marketing practices that capture personal information or make undisclosed and overbroad inferences about individuals. The impact of any unlawful campaigns could draw unwanted regulatory scrutiny in the U.S. and abroad.

- **Cybersecurity**. Security is always a top concern. With every AI-driven marketing campaign, assess the risk that the same content and technology can be used to create unauthorized deep fakes that can inflict both reputational and financial harm to your brand. Be ready to swiftly respond to unlawful visual or audio content.
- **Bias and discrimination**. Depending on the underlying training model, technology, or platform, inherent biases based on the data training set can lead to discriminatory outcomes, determinations, or predictions. As part of your legal review, be sure to assess how the risk of bias and unlawful discrimination was addressed technically, especially in culturally sensitive campaigns.

### 4. Organizational Measures

- **Pilot projects**. Start small before going big. Build a suitable framework that is adequate for your company size, industry vertical, and company culture. Involve a broad group of stakeholders in developing that framework, and test it in controlled environments before wide-scale deployment.
- **Board-level buy-in**. Legal is not the only risk to consider, but it is certainly an important one. Establish acceptable levels of risk within the Board of Directors or other senior management. Going first certainly presents the potential for big payoffs, but also comes with technical and regulatory risk.
- **Education and training**. Once buy-in and risk tolerances are properly assessed, reduce those to policy and standards, and train against those with your creative teams. Set the expectations about how far you are willing to go in deep fake marketing in the near future, and how you will periodically reassess your posture in light of the legal and regulatory landscape.
- **Insurance**. Insurance is a risk mitigation tool. Understanding the role insurance plays in your AI-driven marketing strategy (self-insured vs. covered event), however, is also important. Involve your risk officer, broker, or carrier in evaluating whether your current coverages would cover any claims in the context of deep fake marketing. Again, this area is still poorly understood, and events that result in potential liability remain open to broad and unpredictable interpretation.
- **Explainability**. At every turn, promote transparency in your practices. Within the contract or within the content, avoid deception or dark patterns that could result in legal liability or regulatory scrutiny.

In sum, deep fakes offer advertisers countless opportunities to re-create iconic moments, reuse or enhance existing content, or create entirely fictional characters that result in viral and memorable deep fake campaigns. As deep fake technology continues to advance, however, the need for guardrails, countermeasures, and security controls becomes crucial. From technological solutions that can detect unauthorized deep fakes to legal frameworks that deter malicious use, a proactive approach to potential legal risks is necessary. Developing an overall understanding of the potential severity for a flawed deployment, as well as the likelihood of those consequences being applied to your specific situation, are the key elements to balancing your scorecard.

For now, balancing these new marketplace developments against long-established legal principles will forge a path forward for us in AI-enabled synthetic marketing.

***Harry A. Valetk*** *is a partner at Loeb & Loeb's privacy, security, and data innovations practice group based in New York. He focuses his practice on delivering commercially practical advice to companies of every size on privacy, deep fake and cybersecurity incident response support, and deployment of generative artificial intelligence. He can be reached at hvaletk@loeb.com.* ***Tal Dickstein*** *is a partner at Loeb & Loeb's New York office. He is an entertainment and intellectual property litigator focused on helping clients in the music, motion picture, and advanced media sectors. He can be reached at tdickstein@loeb.com.*