wiley

ARTICLE

Deepfakes, Deep Claims: Using Intellectual Property to Combat Artificial Intelligence's Digital Deception

The Computer & Internet Lawyer
November 24, 2025

This article was originally published by The Computer & Internet Lawyer *and can be viewed here.*

The prevalence of content generated by artificial intelligence (AI) tools has exponentially grown over the past couple of years. Today, 34 million AI-generated images are created daily online. In the social media
space, 71% of images are now created by AI technology.

As AI tools continue to advance, a troubling phenomenon is rapidly emerging: deepfakes. Deepfakes are videos, audio clips, or images generated by artificial intelligence "that convincingly [mimic] a specific individual's likeness or voice." These digital forgeries are often so realistic that they can easily deceive viewers.

For example, in early 2024, the London-based architecture firm Arup was targeted by a deepfake video call in which the voice of the company's chief financial officer was convincingly replicated, resulting in the unauthorized approval of a $25.6 million transaction.

Another incident occurred after Russia invaded Ukraine, when a deepfake video of the Ukrainian President Volodymyr Zelenskyy circulated online, falsely urging Ukrainian soldiers to lay down their arms and surrender.

These cases highlight the profound commercial and political risks posed by deepfakes.

Authors

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law

Practice Areas

Artificial Intelligence (AI)
Copyright
Cybersquatting & Internet IP
Federal Policy and Regulation
Intellectual Property
Intellectual Property
Privacy, Cyber & Data Governance
Trademark

FEDERAL AND STATE LEGISLATION

Until recently, there was no federal legislation to specifically address deepfakes. However, in May 2025, President Trump signed the Take It Down Act into law. The law addresses the online publication of nonconsensual intimate images of adults and minors and describes "digital forgery" as an intimate visual of an individual "created through the use of software, machine learning, artificial intelligence, or any other computer-generated or technological means."

The Take It Down Act changes the landscape of AI-generated and deepfake content in three significant ways.

First, the bill criminalizes publication of sexually explicit non-consensual or deepfake content. An individual who knowingly publishes digital forgery of an adult may be fined under Title 18 of the U.S. Code and imprisoned for up to two years. If the digital forgery depicts a minor, the individual can be fined under the same code and imprisoned for up to three years.

Second, the Act mandates the creation of a notice-and-takedown removal process for social media and other websites. Within one year of enactment, these service providers must create a medium through which reported non-consensual intimate imagery must be taken down within forty-eight hours.

Third, the Federal Trade Commission (FTC) is named as the enforcing agency of the Act's provisions. The FTC has the authority to file civil claims against platforms or websites that do not comply with the bill – though, significantly, the Act does not otherwise create a civil cause of action for private parties.

Additionally, some states have taken steps to address deepfakes. One leading example is Tennessee. A recent amendment to Tenn. Code Ann. § 47-25-1105 makes a person "liable to a civil action if the person publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's voice or likeness, with knowledge that use of the voice or likeness was not authorized by the individual." The amendment defines "voice" to include an "actual voice or a simulation of the voice of the individual."

In contrast to Tennessee's generalized statute that applies to deepfake producers and hosts, many states only have laws addressing deepfake-like situations in the pornography and election realms. For instance, California enacted A.B. 602 in 2020 to afford victims private remedies against those who either create or distribute falsely created and nonconsensual sexually explicit material.16 Florida, Virginia, New York, Indiana, and Washington have all enacted similar laws to address deepfake pornography. And, Pennsylvania recently amended an existing deepfake pornography statute to establish criminal penalties for non-consensual digital impersonations of all types.

Deepfakes in the election space are very concerning as well. Candidates and their supporters can use deepfakes to affect voting outcomes. A recent example is the deepfake of President Joe Biden, which circulated around New Hampshire households in January 2024. The deepfake was a fake telephone voice message instructing people not to vote in the presidential primary. A few states have enacted laws to address these types of election issues. California's A.B. 730 law and Texas' S.B. 751 law both criminalize the creation and dissemination of videos that falsely depict candidates for public office.

Unfortunately, deepfakes are expanding far beyond the pornography and public election arenas. Deepfakes can be used against any individual, business, or other entity as a method of personal or business impersonation. Additionally, deepfakes of celebrities, politicians, chief executive officers, and other public figures can spread false information. This can lead to embarrassment or reputational harm for the impersonated individuals and businesses.

INTELLECTUAL PROPERTY LAWS AND DEEPFAKES

An alternative path to fighting against deepfakes is through intellectual property (IP) laws. A plaintiff may bring a copyright infringement claim if they are the owner of an image, audio, video or other protected work that has been copied to create a deepfake. Similarly, a plaintiff may bring a trademark infringement claim if their mark is improperly used in a deepfake, which could include a product or a person's name.

Plaintiffs may assert these types of IP causes of action not only against the actual creator of the deepfake, but also against "intermediary website operators who knowingly host the misleading content." With respect to the latter, this is particularly important in instances where it is not possible to locate the original creator of the deepfake. Often, the creator of the deepfake is anonymous and/or is in a foreign country. In these situations, the plaintiff can potentially bring legal action against service providers that are being used by the direct infringer to display, distribute or otherwise propagate the deepfake. Thus, IP claims can be a critical tool for deepfake victims even when the original creator of the deepfake cannot be identified.

To hold a service provider liable for hosting an infringing deepfake, the plaintiff must first establish direct trademark infringement or copyright infringement, then establish secondary infringement. To establish a direct trademark or copyright infringement, a plaintiff must prove that the defendant engaged in active and volitional conduct that "can reasonably be described as the direct cause of the infringement." When bringing these claims against service providers, it is critical that a plaintiff show the service provider's role in relation to the deepfake (e.g., hosting) and sufficient knowledge of the infringement. In relation to copyright infringement claims, the service provider may raise one or more of the DMCA safe harbors as an affirmative defense.

The safe harbor provisions of the DMCA provide protection for service providers and incentivize collaboration in taking down copyright-infringing content. Section 512 of the DMCA provides four different safe harbors that limit a service provider's liability for infringing materials. Generally, three conditions must be met for a service provider to qualify for a DMCA safe harbor.

First, the service provider must meet the definition of a service provider – defined as "a provider of online services or network access, or the operator of facilities thereof."

Second, the provider must adopt and reasonably implement a policy that terminates the activity of repeat infringers on the site.

Third, the provider must accommodate standard technical measures.

Notice and takedown requests can be the first step in taking down infringing content, including deepfakes, from a service provider's platform. The process is a key element of the design of the DMCA to promote the "cooperation among Internet service providers and copyright owners." If the notice and takedown process is not successful in removing the infringing content, a copyright owner seeking the removal of content can consider filing suit arguing that the unsuccessful notice provided the service provider with knowledge of the infringement.

SECONDARY INFRINGEMENT CLAIMS

Although two types of secondary infringement claims exist, asserting a claim against a service provider for hosting an infringing deepfake would more typically be framed as a contributory infringement claim. Whereas vicarious liability requires proof of the defendant's actual responsibility over the infringement, contributory liability requires proof that the defendant's actions facilitated the infringement.

Both contributory trademark infringement and contributory copyright infringement have a knowledge requirement: that the defendant must have had "knowledge of specific infringers or instances of infringement." The plaintiff does not need to prove the defendant had specific intent for their website to be involved in infringement. Rather, if the defendant had knowledge of specific infringing activity on its website, and did not take appropriate steps to stop it, a court may find this sufficient to establish contributory liability.

In *Louis Vuitton v. Akanoc Sols*, the U.S. Court of Appeals for the Ninth Circuit upheld a finding of both contributory copyright infringement and contributory trademark infringement against service providers. In that case, Louis Vuitton sent defendants notices regarding products posted on its websites that Louis Vuitton believed infringed its copyrights and trademarks. After receiving the notices, defendants did not take further action to address the infringement. The court rejected the defendants' argument that the jury should have been instructed to make a finding that defendants intended to contribute to the infringement. Rather, the court held that intent was imputed from the defendants' "knowing failure" to prevent infringement.

CONTRIBUTORY TRADEMARK INFRINGEMENT

As set forth by the Supreme Court in *Inwood Labs v. Ives Labs*, if one "continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement," they may be liable for contributory trademark infringement. To establish a claim of contributory trademark infringement, courts consistently require plaintiffs to prove the defendant knew of specific trademark infringers or instances of trademark infringement, then did not take sufficient steps to stop the infringement.

For instance, in *1-800 Contacts v. Lens.com*, the U.S. Court of Appeals for the Tenth Circuit found Lens.com could potentially be liable for contributory trademark infringement. In that case, Lens.com knew that at least one of its affiliates was infringing on 1-800's service mark in its ads but did not make any effort to stop the ads. The court held that there is no requirement for a service provider to have actual knowledge of the identity of the infringer. Because Lens.com could have stopped the infringement without having to know the specific identity of the infringer, this satisfied the knowledge element under Inwood for pleading purposes.

Similarly, in *Rosetta Stone Ltd. v. Google, Inc.*, the U.S. Court of Appeals for the Fourth Circuit reversed the district court's entry of summary judgment on the plaintiff's contributory infringement claims, finding that the evidence presented by Rosetta Stone was sufficient to create an issue of material fact. Rosetta Stone presented a spreadsheet it sent to Google, which reflected the dates of each time Rosetta Stone advised Google that a sponsored link was infringing. The court found this to sufficiently supply Google with specific instances of infringement and therefore created a question of fact "as to whether Google continued to supply its services to known infringers."

In contrast to Rosetta Stone and 1-800 Contacts, in *Tiffany v. eBay*, the U.S. Court of Appeals for the Second Circuit affirmed a finding that eBay was not contributorily liable for trademark infringement because Tiffany did not provide eBay with notice of particular sales listings of counterfeit goods. Instead, Tiffany only provided eBay with general notice that some sellers were selling counterfeits. Because Tiffany did not demonstrate the provider "was supplying its service to individuals who it knew or had reason to know were selling counterfeit Tiffany goods," it failed to satisfy the Inwood knowledge requirement. The court held that "[f]or contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods," rather, "[s]ome contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary."

CONTRIBUTORY COPYRIGHT INFRINGEMENT

The necessary proof to hold a service provider liable for contributory copyright infringement is similar to that of contributory trademark infringement; however, the elements slightly differ. Courts require a showing of the defendant's knowledge of the direct copyright infringement and the defendant's material contribution to the direct copyright infringement. The knowledge element is similar to the knowledge requirement for contributory trademark infringement cases, but the "material contribution" element is more unique to contributory copyright infringement cases.

The Ninth Circuit, in *A&M Records v. Napster*, addressed the knowledge requirement of a contributory copyright infringement claim, finding that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement" and, "[c]onversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."

In *ALS Scan, Inc. v. Steadfast Networks*, the Ninth Circuit rejected plaintiff's contributory copyright infringement claim, finding that the notices it sent to Imagebam.com were general notices that infringement of their images would occur, rather than notice of specific acts of infringement. In contrast, in Greer v. Moon, the Tenth Circuit affirmed a contributory copyright infringement finding because the plaintiff sent multiple requests to the host of the website Kiwi Farms to take down specific books and songs from the website protected by copyright, and even pointed to the locations where the works were being copied.

The material contribution element of a contributory copyright infringement claim generally requires the service provider to facilitate copyright infringement. The Ninth Circuit, in Perfect 10, stated the standard for material contribution for "a computer system operator" to be that it has "actual knowledge that specific infringing material is available using its system . . . and can take simple measures to prevent further damage to copyrighted works . . . yet continues to provide access to infringing works." In practice, this standard is similar to that for contributory trademark infringement liability.

RECENT CASES ADDRESSING AI GENERATED CONTENT

In March 2025, the U.S. District Court for the District of Massachusetts addressed a dispute between two AI dental companies in *Overjet, Inc. v. VideaHealth, Inc.* Both companies use AI tools to scan dental and radiographic X-rays to detect dental diseases.49 As both companies grew in 2023, Overjet claimed that Videa began copying the IP visualization tools, namely the coloring and shape conventions created by Overjet to read scans.50 In February 2024, Overjet filed a number of IP claims against Videa, including copyright and trademark infringement, unfair competition, and direct and indirect patent infringement. Videa claimed that Overjet was not entitled to copyright protection of common colors and shapes because they were not sufficiently original. The court disagreed and found that Overjet's AI software has at least "some minimal degree of creativity" with design choices that serve more than just a functional purpose. Thus, Overjet's claim of copyright infringement survived Videa's Motion to Dismiss.

A month later, in April 2025, the court in *Barkley & Associates, Inc. v. Quizlet, Inc.* confronted the issue of application of IP claims to AI-generated content. In Barkley & Associates, a nurse practitioner continuing education company, sued Quizlet, a study tool platform, for copyright infringement. A Quizlet corporate witness admitted that the company did not independently create their own AI software. Instead, it was made by combining preexisting materials. Barkley alleged that Quizlet infringed its copyrights when it [fed] Barkley's materials to an AI tool to generate Quizlet AI. The court determined that, at the pleading stage, Barkley had pled sufficient allegations to support a theory of direct infringement. To properly assert this type of claim, a plaintiff must plead that an AI model used copyrighted materials to create outputs that were substantially similar to the materials at issue.

In contrast to the above two decisions, in July 2025, the court in Lehrman v. Lovo, Inc. dismissed trademark and copyright claims in a putative class action related to AI-generated voice clones. The trademark claims were dismissed based on inter alia the court's finding that the plaintiff's voices were not protectable marks under the Lanham Act. The copyright claims were dismissed based on the court's finding that copyright "protection does not extend to this kind of imperfect mimicry." Although the trademark and copyright claims were dismissed, the court denied the motion to dismiss as related to state right of publicity claims, finding "construing the Civil Rights Law to exclude digital clones would frustrate the statutory purpose, and, for all practical purposes, enable commercial entities to appropriate individuals' identities without restraint."

CONCLUSION

Deepfakes pose a serious threat – not only to the individuals or businesses who are impersonated, but also to society at large through the spread of misinformation. Intellectual property claims, including right of publicity claims, offer a powerful means to combat deepfakes. These tools are especially effective when the creator of

a deepfake cannot be identified, as claims can be asserted through secondary infringement against those involved in distributing the deceptive content. By leveraging IP laws, organizations and individuals can take meaningful steps to curtail the damage inflicted by deepfakes.