Audio Deepfakes – An Emerging Threat

DANIELLE VAN LIER, Assistant General Counsel, Intellectual Property & Contracts at SAG-AFTRA

The rise of deepfake technology — AI-generated audio and video — has brought with it a range of opportunities, from creating entertaining content to aiding those who cannot speak to committing malicious acts against people and companies. Troubling uses of deepfake video technologies have regularly graced the headlines, particularly in the context of nonconsensual nudity. There has been far less coverage of audio deepfakes, which can be used to commit fraud and other business-directed crimes or even to entertain.

Audio deepfakes got some coverage in mid-2019, when cybersecurity firm Symantec reported at least three incidents in which audio deepfakes were used to fool corporate finance officers into transferring large sums of money into the scammers' accounts.[1] In the U.K., a CEO was defrauded by a convincing voice fake into transferring €220,000 (approx. $243,000) to a Hungarian supplier's bank account.[2] He believed the request came from the parent company's chief executive and did not grow suspicious until the third call during which certain facts relating to the transfer did not line up.[3]

The issue is once more in the spotlight for two very different reasons. The first came in January, when the FTC held its first public workshop on audio cloning technology, including discussions of its ethics, its pros and cons, and authentication, detection, and mitigation.[4] The panel discussed how deepfakes have simplified communication-focused crimes that have historically been difficult to pull off and how, as the technology improves, these type of crimes will continue.[5] The panel also looked at beneficial uses of the technology, which have driven much of their development, including creating synthetic voices for people who lose their ability to speak.

---

[1] Scott Ikeda, "The Cutting Edge of AI Cyber Attacks: Deepfake Audio Used to Impersonate Senior Executives," *CPO Magazine* (July 18, 2019), https://www.cpomagazine.com/cyber-security/the-cuttingedge-of-ai-cyber-attacks-deepfake-audio-used-to-impersonate-senior-executives accessed Aug. 10 2019

[2] Catherine Stupp, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," *The Wall Street Journal* (Aug. 30, 2019), https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402;

[3] Jesse Damiani, "A Voice Deepfake Was Used To Scam A CEO Out Of $243,000," *Forbes (*Sept 3, 2019), https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#353235912241

[4] "FTC You Don't Say: An FTC Workshop on Voice Cloning Technologies," *Federal Trade Commission* (Jan. 28, 2020), https://www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies

[5] Kim Lyons, "FTC says the tech behind audio deepfakes is getting better," *The Verge* (Jan 29, 2020), https://www.theverge.com/2020/1/29/21080553/ftc-deepfakes-audio-cloning-joe-rogan-phone-scams

The next was more recent, when rapper Jay-Z's company, Roc Nation, attempted to use YouTube's copyright takedown procedures to remove videos created by a user called Vocal Synthesis.[6] The channel features AI-generated audio tracks of famous individuals — including past presidents, singers, and actors — reciting excerpts from a wide variety of works ranging from Shakespeare's and Tolstoy's classics to modern animated shows like *South Park* and *Rick and Morty*.[7] YouTube removed and then quickly restored the works and removed the copyright strike against the creator.[8] A complete analysis of legal issues with videos like those created by Vocal Synthesis is beyond the scope of this short piece; however, there does not appear to be any viable basis for a copyright infringement claim with audio deepfakes, which are wholly synthetized new works. While the AI algorithms do utilize copyrighted works to analyze voice patterns and create new works, there is little indication that any of the exclusive rights protected by copyright have been infringed in this context.[9] In some contexts, other legal theories might provide more viable recourse, including defamation, false light, or right of publicity. Vocal Synthesis has been careful to identify videos as "Speech Synthesis," which would likely defeat the falsity element of a defamation claim. False light, while similar to defamation, requires the depiction be highly offensive to a reasonable person — a standard the Vocal Synthesis videos are unlikely to meet. Additionally, a public figure will have to prove the video was created with reckless disregard. Similarly, while California's common law right of publicity is quite broad (requiring simply an unconsented use of the plaintiff's identity for the defendant's advantage and resulting injury), even its elements would be hard to prove in the context of Vocal Synthesis' videos.

From a practical standpoint, as these AI-driven audio cloning technologies improve and become more widespread, companies and high-profile individuals need to start considering them in their security and incident response plans. Companies would be well served to put safety protocols in place, much as many have done to guard against more traditional phishing schemes or business email compromise attacks. For example, a company may choose to implement a multi-step process to verify the authenticity of financial transaction requests. Additionally, as with any other cybersecurity incident, companies should have a process in place to respond, should they fall victim. Because deepfakes can be used to make it appear an individual has said something they never said, which can have devastating impact on an individual's or company's reputation, a public relations strategy should be part of any incident response plan.

---

[6] Ben Beaumont-Thomas, "Jay-Z takes action against 'deepfakes' of him rapping Hamlet and Billy Joel," *The Guardian* (Apr. 29 2020), https://www.theguardian.com/music/2020/apr/29/jay-z-files-takes-action-against-deepfakes-of-him-rapping-hamlet-and-billy-joel
[7] "Vocal Synthesis," *Youtube*, https://www.youtube.com/channel/UCRt-fquxnij9wDnFJnpPS2Q/videos
[8] "Barack Obama and Donald Trump read a special message from this channel's creator (Speech Synthesis)," *Youtube* (Apr. 26, 2020), https://www.youtube.com/watch?v=vk89hEhst88&feature=youtu.be
[9] With video deepfakes, an argument can be made that rights in the underlying work that has been digitally recreated has been infringed, although the deepfake creators may have a strong fair use argument.