Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Deepfake Best Practices Amid Developing Legal Landscape

By **Rod Ghaemmaghami and John Villafranco** (April 16, 2021, 4:55 PM EDT)

Rod Ghaemmaghami

John Villafranco

I'll believe it when I see it. In 2021, you can't say this with confidence.

As artificial intelligence technology has substantially improved over the past few years and as digital editing applications have become more accessible directly to consumers, synthetic media and deepfakes are altering what we see and what we hear.

Last month, Mountain Dew used deepfake technology to digitally resurrect the deceased. A new episode of Bob Ross' TV show, "The Joy of Painting," was created and aired on YouTube, showing Ross, who died in 1995, painting a scene that included a Mountain Dew bottle.

Beyond the ethical questions these types of uses raise, there are also legal implications to consider. Some states have begun enacting laws that protect victims of nonconsensual pornography from deepfake technology and that restrict the use of deepfake technology in election interference.

State laws already in existence may be used if biometric data is within the scope of what is regulated.

The technology behind deepfakes offers new and innovative ways to create advertisements and to engage target audiences. It is already being used commercially. As this technology is still relatively young and in the early stages of commercial adoption, we should set a standard of best practices to protect against harmful uses and to ensure compliance with laws in existence and pending.

The Rise of Synthetic Media

A deepfake "is a type of 'synthetic media,' meaning media [including voice, picture, video] that is either manipulated or wholly generated by AI," according to author Nina Schick.[1]

The technology itself, deep machine learning and self-competing AI, is impressive.[2] There are social benefits such as protecting the identities of whistleblowers or victims, rendering synthetic voices for individuals who have lost their voices, providing closure to a grieving mother, although synthetic

resurrection carries its own ethical issues.

The debate, however, is ongoing: Is this technology so dangerous that its potential harms outweigh its benefits? Ninety-six percent of deepfake videos are of nonconsensual porn.[3]

And people may be most familiar with its political uses: A video of U.S. House of Representatives Speaker Nancy Pelosi, D-Calif., slurring her words was circulated in 2019 for the purpose of deception,[4] and video of former President Barack Obama speaking about former President Donald Trump was made by filmmaker Jordan Peele to raise awareness.[5]

Additionally, elder fraud and scams are highly likely with synthetic voice, image and video. The debate will continue as this technology advances.

Use of Deepfake Technology in Advertising

Deepfake technology has already made its way into the toolkit of the market. While commercial use has only just started, there are innovative advertising use cases. Two types of use cases have arisen.

First, celebrities and influencers may license their likeness, their voice and their face to brands. A computer can then take a voice or face and reproduce it in dozens of different languages and poses. This means more impact for each advertisement, easier performance for celebrities and influencers, and more control by the brand on the final product.

- In 2020 amid the COVID-19 pandemic, Hulu created an advertisement of athletes cooking, painting and playing instruments to announce that Hulu has live sports again.[6] But the athletes were never actually filmed cooking, painting or playing instruments; that was deepfake technology used to impose the athletes' faces onto bodies of others doing those activities.

- In 2019, a malaria awareness advertisement featured British soccer player David Beckham speaking nine languages. It showed how deepfakes can broaden the reach of a public message, receiving 400 million impressions globally within two months.[7]

- Zao, an app released in China, allows users to star in their favorite movies by seamlessly superimposing their face onto actors' bodies in well-known movie scenes.[8]

Second, deepfake technology can be used in commercial industries to personalize experiences. For example, in the fashion industry, it can be used to help people see clothes on models that look more like them. Deepfakes can "show outfits on a broader variety of models of different skin tones, heights, and weights," according to Vogue Business.[9]

- In 2020, Reface AI enabled app users to virtually try on Gucci clothes as part of a trial with French luxury brand Kering, resulting in 1 million swaps in a single day.[10]

- AI company Tangent.ai is seeking to capitalize on this with an algorithm designed to help consumers determine which products will look good on them. For example, a consumer may change a model's lipstick, hair color, ethnicity or race.[11]

Both of these types of uses of deepfake technology present legal challenges.

Legal Tools

The legal framework around deepfake technology is still developing. Some states have enacted legislation that will protect against harmful uses. Additionally, there are laws that can indirectly be applied toward the harmful use of deepfake technology.

For nonconsensual porn, for example, there are not a lot of legal options. While, in the U.S., 46 states have banned revenge porn, only California and Virginia include protection against faked and deepfake media.[12]

State laws that protect against deepfake technology:

- California passed two laws in 2019. California Civil Code Section 1708.86 creates a private right of action against a person who creates or intentionally discloses sexually explicit material that wasn't consented to.[13] California Code of Civil Procedure Section 35 prohibits a person, committee or entity from distributing with actual malice a "materially deceptive audio or visual media" of a candidate on the ballot.[14] This law protects against deepfake use in elections.

- Texas Election Code Chapter 255 prohibits the use of deepfakes for election interference.[15]

- Virginia amended criminal law on revenge porn to include deepfake images and video.[16]

- Other states, such as Hawaii, have introduced bills to protect against deepfake images whether for unlawful use, nonconsensual pornography, or election interference.[17]

The federal government has attempted to legislate deepfake technology in recent years as well. Some bills have stalled, such as the Deepfakes Accountability Act[18] and Deepfakes Report Act.[19]

Others have passed into law, such as the Identifying Outputs of Generative Adversarial Networks Act,[20] which directs the National Science Foundation and the National Institute of Standards and Technology to support research for the development of measurements and standards of the technology behind deepfake media.

The federal government also included restrictions on the use of deepfake technology, through the National Defense Authorization Act in 2020,[21] restricting the use of deepfakes for foreign influence and weaponization.

State laws that don't directly define deepfake technology may be used to protect against it:

- The Illinois Biometric Information Privacy Act was enacted in 2008 and regulates the collection and storage of biometric information. Biometric information is defined as including "voice recognition [and] facial-geometry recognition," which may overlap with the technology used in deepfake and synthetic media.[22]

- The California Consumer Privacy Act includes biometric information as personal information, and includes "face … voice recording … faceprint, voiceprint."[23] Other privacy bills are currently pending.

- The Virginia Consumer Data Protection Act, which was recently enacted into law, also regulates biometric data. However, it excludes in its definition of biometric data "a physical or digital photograph, a video or audio recording or data generated."[24]

At the regulatory stage, the Federal Trade Commission held a workshop on voice cloning technologies in January 2020. Academics, regulators and industry members spoke about both the positive and the negative potential and actual use cases for deepfake media — whether voice, picture or video.

The workshop highlighted potential areas of concern — such as grandparent and phishing scams, unauthorized use of likeness and cyberstalking — and ultimately panelists repeatedly recommended that the main preventative measure from these harms is awareness. Awareness that this technology exists and is realistic can help protect against harm.

Solutions

Synthetic media and deepfake technology raise a host of legal, ethical and technological issues. For commercial and noncommercial uses, we need a system that (1) recognizes and detects synthetic media, (2) labels media as synthetic, and (3) places limits on the type of content this technology should be used for.

- Detection: Anti-deepfake tech that could either stop a user from seeing a deepfake video or hearing a deepfake audio, or alert the user of the existence of a deepfake.

- Labeling: Content can be watermarked or signaled as "not real people." Blockchain has potential as a future means of tracking authenticity.[25]

- Content restrictions: Until an ethical framework is developed, and in the absence of standards, we can focus more on regulating the content in which synthetic media is used and not on the presence or absence of it. Fostering synthetic media for uses besides violence, pornography, news or political satire may allow the technology to mature while drawing a clear line between appropriate and inappropriate uses.

Best Practices Going Forward

- To state the obvious, use deepfake technology with the consent of the subject.

- Make it clear to viewers of the media that the content is synthetic and not real.

- Establish limits on the use of a subject's likeness and build in processes for minimization, retention, deletion, etc.

- Watermark your synthetic media so that others can identify your content as synthetic.

- Limit the use synthetic media portraying certain content: violence, pornography or political content.

Rod Ghaemmaghami is an associate and John Villafranco is a partner at Kelley Drye & Warren LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Nina Schick, Deepfakes: The Coming Infocalypse 8 (2020).

[2] If you visit thispersondoesnotexist.com, you can see how realistic it is for yourself. Every time you reload the page an image of a synthetic person (someone who doesn't exist) is shown.

[3] Nina Schick, Deepfakes: The Coming Infocalypse 40 (2020).

[4] Sarah Mervosh, Distorted Videos of Nancy Pelosi Spread on Facebook and Twitter, The New York Times (May 24, 2019), https://www.nytimes.com/2019/05/24/us/politics/pelosi-doctored-video.html.

[5] BuzzFeedVideo, You Won't Believe What Obama Says In This Video!, YouTube (April 17, 2018), https://www.youtube.com/watch?v=cQ54GDm1eL0.

[6] Hulu, Hulu Has Live Sports Again, YouTube (Aug. 13, 2020), https://www.youtube.com/watch?v=50J4VP2AG9o.

[7] Kati Chitrakorn, How Deepfakes Could Change Fashion Advertising, Vogue Business (January 11, 2021), https://www.voguebusiness.com/companies/how-deepfakes-could-change-fashion-advertising-influencer-marketing.

[8] Jason Mueller, Genevieve Perez, "Deepfake" Technology: Very Real Marketing Value … and Risks, 11 The National Law Review (2020), https://www.natlawreview.com/article/deepfake-technology-very-real-marketing-value-and-risks.

[9] Kati Chitrakorn, How Deepfakes Could Change Fashion Advertising, Vogue Business (Jan. 11 2021), https://www.voguebusiness.com/companies/how-deepfakes-could-change-fashion-advertising-influencer-marketing.

[10] See id.

[11] Jason Mueller, Genevieve Perez, "Deepfake" Technology: Very Real Marketing Value … and Risks, 11 The National Law Review (2020), https://www.natlawreview.com/article/deepfake-technology-very-real-marketing-value-and-risks.

[12] Karen Hao, Deepfake Porn is Ruining Women's Lives. Now the Law May Finally Ban It, Technology Review (Feb. 12 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/.

[13] Cal. Civ. Code § 1708.86.

[14] Cal. Civ. Pro. Code § 35.

[15] Tex. Elec. Code § 255.

[16] Va. Code Ann. § 18.2-386.2.

[17] Haw. S.B. No. 1009 (2021).

[18] Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019, H.R. 3230, 116th Cong. (2019).

[19] Deepfakes Report Act of 2019, H.R. 3600, 116th Congress (2019).

[20] 134 Stat. 1150 (2020).

[21] National Defense Authorization Act for Fiscal Year 2020, S. 1790, 116th Cong. (2019).

[22] 740 Ill. Comp. Stat. 14 (2008)

[23] Cal. Civ. Code § 1798.140.

[24] Va. Code Ann. § 59.1-571 (2021).

[25] Kati Chitrakorn, How Deepfakes Could Change Fashion Advertising, Vogue Business (Jan. 11 2021), https://www.voguebusiness.com/companies/how-deepfakes-could-change-fashion-advertising-influencer-marketing.