Deep concerns over political deepfakes

By Ki Hong, Esq., Tyler Rosen, Esq., and Aanchal Chugh, Esq., Skadden, Arps, Slate, Meagher & Flom LLP

MAY 20, 2024

A candidate's voice used in robocalls discouraging his voters from going to the polls for a primary election ...

Synthetic videos of famous actors asking people to vote for the opposition party ...

Faked audio in which a candidate appears to say he will raise the price of beer ...

These are just a few recent examples of deepfakes in politics.

Artificial intelligence (AI) is poised to make the already well-entrenched problem of misinformation in politics significantly worse. Regulators, lawmakers and technology companies are struggling to figure out how to best combat this new high-tech iteration of an age-old staple of politics: dirty tricks.

Unsurprisingly, neither the federal election law nor its regulations directly address deepfakes. Indeed, after receiving a non-profit organization's petition for action, the Federal Election Commission (Commission or FEC) last year sought public comment inviting ideas on how to best regulate deepfakes.

The regulation the Commission eventually promulgates, if any, will have to be premised on the Federal Election Campaign Act's statutory prohibition on a candidate or candidate's agent "fraudulently misrepresent[ing] himself or any committee or organization under his control as speaking or writing or otherwise acting for or on behalf of any other candidate or political party," in a way that is damaging.

As a result, even if the Commission moves forward with a rulemaking, it will have to be limited to candidates and their agents — not third parties like Super PACs and other outside groups that are more likely to employ deepfake technology to run deceptive ads. Thus, to effectively regulate political deepfakes, there will have to be a legislative fix.

While deepfakes are new, regulations bringing transparency to political advertising are not. At the federal level, political advertisements and electioneering communications require a disclaimer identifying who paid for the advertisement or communication and whether or not it was authorized by a candidate.

In theory, these federal disclosure requirements allow the victims of a deepfake attack to identify and sue the sponsor of the ad for libel and, in some cases, the misappropriation of their likeness. While the standard for misappropriation of likeness varies by state, many jurisdictions require proof that the defendant being sued gained a commercial benefit from the use.

The law of appropriation ties back to the law of unfair competition and has historically excluded the unauthorized use of likeness in the context of newsworthy material or legitimate public concern. Thus, given the lack of commercial gain and the newsworthy nature of election-related information, misappropriation of likeness actions may prove to be an uphill battle for victims of such attacks.

Artificial intelligence is poised to make the already well-entrenched problem of misinformation in politics significantly worse.

Similarly, in the context of political speech, libel suits tend to be rather rare and seldom successful because public officials are subject to a higher standard than private plaintiffs. In *New York Times v. Sullivan*, the Supreme Court held that public officials must meet the burden of proof for "actual malice" when suing for libel.

In other words, the burden is on a plaintiff to prove that the facts stated or implied are false, the statement was conveyed to others, the plaintiff was harmed, and that the defendant either knew the statement was false at the time of publication or else published the statement with reckless disregard as to its falsity. A plaintiff may demonstrate reckless disregard in several ways, including through evidence that a defendant relied on sources that they knew to be unreliable, as well as evidence that a defendant purposefully avoided the truth.

While such libel cases may be difficult to prove when a third party is directly making a statement, it may be easier when a person goes out of his or her way to use AI to create a deepfake. For example, creating a deepfake to create a false appearance that the candidate made a statement could be viewed as a knowing and intentional effort to disseminate that falsity. It will be interesting to see how the jurisprudence on such arguments develops.

Although the FEC has not yet taken action to address deepfakes, several states have passed legislation regulating deepfakes. At least 39 states are considering or have passed measures that

would increase transparency with regard to AI-generated deepfake political advertisements.

Similar to the FEC's disclaimer requirements, many states are requiring disclosure on AI-produced content to provide consumers with the ability to recognize synthetic content. For example, Wisconsin's recently enacted AB 664 requires campaign advertisements with audio or video material generated by AI to include a disclaimer that it was generated by AI. In every state that has passed such legislation, the bills have received bipartisan support.

These states generally address the issue with disclaimer requirements rather than prohibitions, because prohibitions on false political advertising have run into constitutional challenges.

For example, Ohio's statute prohibiting campaigns from making false statements about a candidate's voting record, or knowingly or recklessly making false statements about a candidate to help a candidate win or lose an election was struck down in 2016. The 6th U.S. Circuit Court of Appeals in *Susan B. Anthony List v. Driehaus* found that the prohibition violated the First Amendment and the Fourteenth Amendment as content-based restrictions on political speech not narrowly tailored to address a compelling government interest in fair elections. Governments have limited authority to regulate the substance of political advertisements because voters have a right to uncensored information from candidates and are presumed to be able to evaluate such information themselves before making decisions at the ballot box.

However, similar to libel cases, once AI-generated deepfakes are introduced into the mix, this constitutional paradigm may no longer hold given the compelling government interest that may be demonstrated by the heightened threat that deepfakes pose to fair elections. There is a difference in-kind between a person making potential false statements about a candidate and a deepfake intentionally attempting to make it appear that the candidate is making that statement.

Social media platforms and other private companies, on the other hand, have a freer hand in controlling this space than the government. Given the expertise certain of them have in AI, it is perhaps unsurprising that many technology companies are urgently attempting to address the issue of deepfakes by releasing new, or altering existing, policies.

While some social media platforms, such as TikTok, LinkedIn, and Pinterest, have banned political advertisements altogether, others are confronting the issue of deepfakes specifically. Last February, several companies, including Microsoft, Meta, Google, and Amazon, announced a new "A Tech Accord to Combat Deceptive Use of AI in 2024 Elections." (https://bit.ly/3UYkdZE) The goal of the policy is to prevent the spread of videos, audios, and images that fake or alter the likeness of political candidates, election officials, and other key political stakeholders.

In addition, Meta released a new policy last year that requires political advertisers to disclose when they use altered or digitally created media. In a blog post, Meta said it would require advertisers to disclose during the ad-buying process "whenever a social issue, electoral, or political ad contains a photorealistic image or video, or realistic sounding audio, that was digitally created or altered." The policy stops short of banning altered media altogether — conceding that AI-generated media is here to stay. "Helping People Understand When AI Or Digital Methods Are Used In Political or Social Issue Ads," Facebook.com, Nov. 8, 2023, Updated Jan. 3, 2024. (https://bit.ly/3ylcKLD)

Although the FEC has not yet taken action to address deepfakes, several states have passed legislation regulating deepfakes.

Similarly, in September 2023, Google revised its political advertising policies to require politicians to disclose if they use any "synthetic" or AI-generated content in their ads featured on Google's platforms. While Google already banned outright "deepfakes" that aim to deceive voters, their new policy requires companies to disclose any use of the technology beyond minor edits such as adjusting color or contrast in an image.

Under the policy, politicians are required to include a label in all their ads that contain synthetic content. However, ads containing synthetic content altered in a way that is inconsequential to the claims made in the ad will be exempt from such disclosure requirements.

While private companies, state legislatures, and the FEC have provided some framework to navigate and control political deepfakes, it is clear that the First Amendment protections on political speech make it difficult for public officials and states to gain recourse or enforce prohibitions against false political advertisements. Despite diverse actors attempting to gain some control in the space, a nationwide restriction on deepfakes has yet to be passed and multiple stakeholders have voiced opposition to the prospect of such comprehensive legislation.

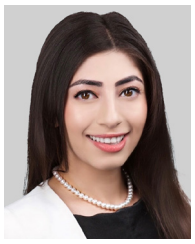
With many democracies around the world heading to the polls this year, the role of AI in politics is an issue of global concern that extends beyond the U.S. Some countries, such as China, have put regulations in place addressing the emerging technology, while other parts of the world, such as India and the European Union, are grappling with how to regulate a technology that is moving at a speed faster than the legislative process is equipped to govern.

While the future of regulations is undetermined, one thing is certain: AI-generated information is not going anywhere.

Ki Hong is a regular contributing columnist on political law for Reuters Legal News and Westlaw Today.

About the authors





Ki Hong (L) is a partner at **Skadden, Arps, Slate, Meagher & Flom LLP** and head of the firm's political law compliance and investigations group. He advises major corporations on the unique political law issues they face when engaging in government affairs or government procurement activity. He is based in Washinton, D.C., and can be reached at ki.hong@skadden.com. **Tyler Rosen** (C) is a counsel at the firm in the political law compliance and investigations group. He advises clients on pay-to-play, campaign finance, lobbying, and gift and conflict of interest compliance matters at the federal, state and local levels and on ESG considerations in the political law space. He can be reached at tyler.rosen@skadden.com. **Aanchal Chugh** (R) is an associate at the firm in the political law compliance and investigations group. She can be reached at aanchal.chugh@skadden.com.

This article was first published on Reuters Legal News and Westlaw Today on May 20, 2024.