

October 16, 2023

Federal Election Commissioners Federal Election Commission 1050 First Street, NE Washington, DC

Fraudulent "Voice" and Perspective in Ads: Campaign for Accountability's Comment on (REG 2023-02) -- Artificial Intelligence in Campaign Ads

Dear Commissioners,

On behalf of Campaign for Accountability (CfA)—a nonprofit watchdog group which, separately, works to highlight campaign finance violations and conducts research around harms stemming from unregulated online advertisements—I'm writing to urge the Commission to take seriously concerns raised by Public Citizen in its Petition for Rulemaking.

I trust that the Commission understands the potential for harm that deepfakes pose in exacerbating disinformation and fraud in campaign ads. However, there is clearly some doubt amongst at least several Commissioners that: a) the harm is not better mitigated by the private sector b) the potential for harm is novel or unique to existing methods of manipulating information, and c) that the Commission even has jurisdiction to enforce deepfake fraud.

Before addressing each of those points, I will first suggest a slightly narrower version of Public Citizen's request, which I believe may help bridge the gap in understanding between those who do and those who do not believe the FEC has jurisdiction over this matter. While Public Citizen made very clear *in its arguments* that the novel danger that deepfakes pose as a tool for electoral manipulation is in their ability **to speak** *for or on behalf of someone else*, we respectfully do not believe the Petition's concluding recommendation makes this sufficiently clear.¹

Therefore, we'd suggest a slight narrowing of the language used in Public Citizen's concluding recommendation, asking the Commission: "... to specify in guidance as well as in an amendment to 11 C.F.R. §110.16(a) that if candidates or their agents fraudulently misrepresent adopt the voice of other candidates or political parties through deliberately false AI-generated content in campaign ads or other communications..."

I hope that you keep this distinction front of mind as you consider these arguments.

¹ Public Citizen, "Second Submission: Petition for Rulemaking to Clarify that the Law Against "Fraudulent Misrepresentation" (52 U.S.C. §30124) Applies to Deceptive Al Campaign Communications," July 13, 2023, available at https://sers.fec.gov/fosers/showpdf.htm?docid=423502.

Absent Compulsion, Online Platforms Will Not Sufficiently Police Ads

In previewing his initial thoughts on the FEC's role in regulating AI in campaign ads during a September 20 hearing before the Committee on House Administration, Commissioner Sean Cooksey said, "private entities are free to impose their own limits and disclosure requirements on the ads that they host on their own platforms" – hinting that he may be reticent to act until we see how online platforms' labeling of AI-generated content "plays out in practice."²

While it may be tempting to assume that private industry can or will mitigate harm, online ad platforms run by Google and Meta have consistently failed to self-police ad disclaimers when no law or regulation compels their accuracy or consistency.

Google has demonstrated this in its misapplication of abortion-related ads, with a 2022 investigation finding that many ads that Google promised to label lacked vital information.³ For its part, Meta-owned Facebook has long struggled to correctly assign disclaimers to political ads, with researchers in 2021 finding that, "61% more ads are missed than are detected worldwide, and 55% of U.S. detected ads are in fact non-political."⁴

Both examples illustrate how, even when companies decide they will self-police, the lack of accountability for both the platform and the ad creator means that neither has a real incentive to apply labels accurately.

When enforcement is left to the platform—and not the government—bad actors have no deterrent. Surely, someone seriously motivated to spread disinformation is not deterred by the threat of having their Google or Facebook account suspended for breaking platform policy. After all, they need only a new email address and a VPN to make a new account and perpetuate the fraud all over again.

Fraudulent presentation of fact vs. Fraudulent attribution of voice.

During the Commission's August 10, 2023 open meeting, Commissioner Dickerson stated clearly that he believes that "There is nothing special about deepfakes or generative AI—the buzzwords of the day—in the context of this petition. If the statute reaches fraudulent attempts to show that an opponent "said or did something they did not do" it shouldn't matter how the fraud is accomplished."⁵

² Committee on House Administration, September 20, 2023, Full Committee Hearing: "Oversight of the Federal Election Commission" *available at* https://www.youtube.com/watch?v=Po3jvGO7ib4&t=3943s.

³ Bloomberg, Julia Love and Davey Alba, September 29, 2022, "Google is Still Failing To Label Many Ads From Anti-Abortion Centers," *available at* https://www.bloomberg.com/graphics/2022-google-search-abortion-clinic-crisis-pregnancy-center-ads.

⁴ NPR, Bill Chappell, December 9, 2021, "Researchers explain why they believe Facebook mishandles political ads," available at https://www.npr.org/2021/12/09/1062516250/researchers-explain-why-they-believe-facebook-mishandles-political-ads.

⁵ Federal Election Commission, August 10, 2023, Open Meeting, available at https://youtu.be/IWad5ixSZks?t=102.

He then listed several examples of behaviors that—by his implication—would necessarily fall under the FEC's jurisdiction *if* it were to accept its jurisdiction over fraudulent misrepresentation achieved using AI:

"Lying about someone's private conversations, or posting a doctored document, or adding sound effects in post-production, or manually air-brushing a photograph—if intended to deceive—would already violate our statute."

Respectfully, Commissioner Dickerson's highlighting of these examples displays a fundamental misunderstanding of the argument being put forth—and the nuances of perspective and point-of-view in communication more broadly. In all these scenarios listed, the fraud that is accomplished is in the alteration of *fact*. In contrast, cutting-edge audio or video "deepfake" technology can, uniquely, establish a false *voice* that other methods of forgery cannot.⁶

Yes, it is true that deepfakes *also* involve the changing of fact. But it is indeed the changing of *voice/perspective* that would make certain uses of deepfakes in campaign ads novel in their end effect. To demonstrate this, let's take the first of the Commissioner's examples: "Lying about someone's private conversation."

Imagine an ad in which a narrator delivers the line: "Joe Biden told his rich donors that he wants to abolish the public school system."

To supporters of the President seeing this ad for the first time, the facts presented may seem shocking. Still, that viewer/listener will naturally know that these facts being presented to them are done so through a *third-person's perspective*—specifically, the narrator's perspective. Knowing that this fact is delivered by a third party "voice," the viewer will likely next want to know the identity of that "voice" so that they can judge whether to consider them credible.

Accordingly, Justice Kennedy in his Citizen's United opinion affirmed the importance of "paid for" disclaimers to satisfy the government's informational interest in the identity of the speaker: "The First Amendment protects political speech; and disclosure *permits citizens and* shareholders to react to the speech of corporate entities in a proper way. This transparency enables the electorate to make informed decisions and give proper weight to different speakers and messages."

Next, imagine a deepfake video that appears—with realism capable of passing any reasonable person standard—to show surreptitiously recorded, unbroken and unedited footage of President Biden standing at a podium saying, "I want to abolish the public school system...Seriously... I'm not kidding around." Imagine that there are no cuts in the video that would produce the added "voice" of an editor's hand. There is no added music, nor text overlayed. There is simply the

⁶ The concept of "voice" is not restricted to the literal sound made by someone's vocal cords. Rather, it encompasses every identifying feature one considers when ascribing authorship. i.e. "I wrote the speech in his voice," or "This painter has a very fresh and unique voice."

⁷ Supreme Court Of The United States and Anthony M. Kennedy, Citizens United v. Federal Election Commission, 558 U.S. 310. 2009. available at https://www.loc.gov/item/usrep558310/

first-person "voice" of the President saying that he wants to abolish public schools—with an added "Biden-ism" for good measure.

In a situation like this, where the sole voice appears to be the President's, the viewer does not have that crucial moment where they decide to assess the credibility of the message by determining its speaker. They *already* know (or have at least been tricked into thinking they know) the speaker's identity. And they likely already have an opinion on whether they believe the President to be a credible representative of his own campaign.

I anticipate those aligned with Commissioner Dickerson's view on this matter may again say that the *method* of fraud (in this case, AI) should not be considered—only the end result. But, short of an entire Hollywood visual effects team—spending hours manually editing pixels to accurately line up the President's lip movements to match the words—there is not (and has never been) an alternative to AI deepfake technology in achieving this end result.

Now consider if, instead of using technology or post-production manipulation, this same video was accomplished by using an *impersonator*. What if that impersonator—somehow indistinguishable in appearance and voice—were to knowingly participate in a fakery and pretend to be President Biden with the goal of making the eventual viewers of the video convinced that he—the actor—*is* the President?

In the August 10 hearing, Commissioner Dickerson emphasized that the Commission *does* have jurisdiction over a narrow type of fraud, when "a person [is] fraudulently misrepresenting himself as acting for or on behalf of another candidate." It is not the facts presented, but the speaker's false presentation as an agent of that campaign that matters.

How can any reading of that statue not agree that an impersonator in this situation is not *he himself* fraudulently claiming agency? Just like the deepfake, his identity (his "voice") is the *primary* fraud—whatever facts he is told to say in the filming of this ad come secondary.

This is completely analogous to a deepfake. If there is still disagreement here, then it appears to be caused by a misunderstanding of the process by which a deepfake is created.

A deepfake is not created by magic. To achieve this hypothetical deepfake of President Biden saying something he did not say, presumably the creator will *type into a keyboard* or *speak into a microphone* that fraudulent language. By doing this, Public Citizen explained, this "deepfak*er*" is speaking for, or on behalf of the candidate being deepfaked.⁹

⁸ Federal Election Commission, August 10, 2023, Open Meeting, available at https://youtu.be/IWad5ixSZks?t=102.

⁹ Public Citizen, "Second Submission: Petition for Rulemaking to Clarify that the Law Against "Fraudulent Misrepresentation" (52 U.S.C. §30124) Applies to Deceptive AI Campaign Communications," July 13, 2023, available at https://sers.fec.gov/fosers/showpdf.htm?docid=423502.

advertisement is negated by the presence of a disclaimer at the end of the advertisement. narrow type of fraud—may say that any fraudulent misrepresentation committed during the We anticipate that some—still eager to deny the Commission's jurisdiction over even this

Yet, not all videos that serve as campaign ads have disclaimers.

"promote" that post with campaign cash—without any disclaimer whatsoever. 10 theoretical "abolish public schools" deepfake as an organic post to their Facebook page and then online ad disclaimer guidelines, it may be completely legal for a campaign to upload this Due to the FEC's unfortunate choice to remove "placed or promoted" language from updated

represents the sole voice of a particular candidate, with no disclaimer to suggest otherwise voters to see a deepfake which fraudulently, willfully, and successfully convinces viewers that it In intent and effect, this is the same as a campaign ad. In this scenario, a campaign is paying for

We see no way that this scenario falls outside of the FEC's jurisdiction to hold people accountable for "fraudulent misrepresentation" as defined by 11 C.F.R. §110.16(a). It seems that flaws in once manageable gaps in existing regulations have compounded with emerging may engage in behavior that obviously violates the intent of FEC restrictions. technology in a way that exposes glaring loopholes, creating instances like this where campaigns

the online disclaimer laws to fix the "promoted" loophole so that this flagrant example could not Separate from any discussions around AI, we urge the Commission to consider another pass at be permitted.

suggestion/edit in bold) Citizen—we encourage "the Commission to specify in guidance as well as in an amendment to the restrictions and penalties of the law and the Code of Regulations are applicable." (CfA that the content is generated by artificial intelligence and does not represent real events – then or other communications — absent clear and conspicuous disclosure in the communication itself candidates or political parties through deliberately false AI-generated content in campaign ads Additionally-11 C.F.R. §110.16(a) that if candidates or their agents fraudulently adopt the voice of other repeating a slightly narrowed version of the recommendation proposed by Public

Sincerely,

My chall tupperson the

Michelle Kuppersmith Executive Director

¹⁰ Axios, Lachlan Markay, November 29, 2022, "FEC Scales Back Digital Ad Transparency Rule After Backlash," available at https://www.axios.com/2022/11/29/fec-digital-ad-disclosure-rule