Federal Election Commission
1050 First Street, NE
Washington, D.C. 20463

October 11, 2023

Submitted electronically

Petition for Rulemaking to Clarify that the Law Against "Fraudulent Misrepresentation" (52 U.S.C. §30124) Applies to "Deepfakes" in Campaign Communications

Public Citizen Comment on REG 2023-02

Dear Commission:

Exaggerated campaign ads, sometimes even bordering on outright dishonesty, are nothing new to American politics. Generally, though, it has long been possible for motivated voters and the news media to promptly discern the difference between fact and fiction.

That is now changing.

Extraordinary advances in artificial intelligence (A.I.) now provide political operatives with the means to produce campaign ads and other communications with computer-generated fake images, audio or video of candidates that appear real-life, fraudulently misrepresenting what candidates say or do. Generative artificial intelligence and deepfake technology – a type of computerized technology used to create fake but convincing images, audio and video hoaxes[1] – is evolving very rapidly. Every day, it seems, new and increasingly convincing deepfake audio and video clips are disseminated. And the pace is very likely to pick up as the 2024 presidential election nears.

Campaigns are already running A.I.-generated ads that look and sound like actual candidates and events, but in fact are entirely fabricated. These ads look and sound so real that it is becoming exceedingly difficult to discern fact from fiction.

When A.I.-generated content makes a candidate say or do things they never did – for the explicit purpose of damaging that targeted candidate's reputation – these ads are known as "deepfakes." The practice of disseminating deepfakes in political communications on social media or mainstream television and radio outlets is currently legal in federal elections and most states. These ads are not even subject to a disclaimer requirement noting that the content never happened in real life.

In the recent mayoral election in Chicago, mayoral candidate Paul Vallas complained that AI technology was used to clone his voice in a fake news outlet on Twitter in a way that made him appear to be condoning police brutality.[1] It never happened. Vallas lost the race.
As the 2024 presidential election heats up, some campaigns are already testing AI technology to shape their campaign communications. The presidential campaign of Gov. Ron DeSantis, for example, posted

[1] Megan Hickey, "Vallas campaign condemns deepfake posted to Twitter," CBS News (Feb. 27, 2023), available at: https://www.cbsnews.com/chicago/news/vallas-campaign-deepfake-video/

deepfake images of former President Donald Trump hugging Dr. Anthony Fauci.[2] The hug never happened. The just concluded national elections in Slovakia were marred by late-breaking deepfake audio clips spread over social media,[3] and which may have exerted a decisive influence over the results.[4]

In addition to the direct fraud they perpetrate, the proliferation of deepfakes offers the prospect of a "liar's dividend", in which a candidate legitimately caught doing something reprehensible generates his or her own deepfakes to cover up their actions. It is very difficult to prove a recording is real. Conflicting images and audios of what a candidate said or did could be used to lead a skeptical public to doubt the authenticity of genuine audio or video evidence.[5]

Altogether, the stakes of an unregulated and undisclosed Wild West of AI-generated campaign communications are far more than the impact on candidates; it will further erode the public's confidence in the integrity of the electoral process itself. If voters cannot discern fact from fiction in campaign messages, they will increasingly doubt the value of casting a ballot – or the value of ballots cast by others.

Clarify that Deepfakes Are Covered Under the Law Against Fraudulent Misrepresentation

The Federal Election Commission (FEC) is considering rulemaking to clarify whether and how deepfakes in campaign communications are covered under the law against "fraudulent misrepresentation" (52 U.S.C. §30124). Because of the limitations and narrow reach of the law, such rulemaking should not be viewed as a panacea to the problem of deliberately deceptive AI-content in campaign messages, but it would be a very important first step.

The relevant law that grants the FEC authority to regulate the use of "Artificial Intelligence" in campaign ads is the law against "fraudulent misrepresentation" (52 U.S.C. §30124), which is part of the Federal Election Campaign Act (FECA).

The fraudulent misrepresentation law reads:

> **§30124. Fraudulent misrepresentation of campaign authority**
>
> *(a) In general*
>
> *No person who is a candidate for Federal office or an employee or agent of such a candidate shall-*
>
> *(1) fraudulently misrepresent 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 or*

---

[2] Nicholas Nehamas, "DeSantis campaign uses apparently fake images to attack Trump on Twitter, New York Times (June 8, 2023), available at: https://www.nytimes.com/2023/06/08/us/politics/desantis-deepfakes-trump-fauci.html?auth=login-google1tap&login=google1tap

[3] Olivia Solon, "Trolls in Slovakian Election Tap AI Deepfakes to Spread Disinfo," Bloomberg (Sept. 29, 2023), available at: https://www.bloomberg.com/news/articles/2023-09-29/trolls-in-slovakian-election-tap-ai-deepfakes-to-spread-disinfo.

[4] Morgan Meaker, "Slovakia's Election Deepfakes Show AI is a Danger to Democracy," Wired (Oct. 3, 2023), available at: https://www.wired.co.uk/article/slovakia-election-deepfakes.

[5] Bryan McKenzie, "Is that real? Deepfakes could pose danger to free elections," UVA Today (Aug. 24, 2023), available at: https://news.virginia.edu/content/real-deepfakes-could-pose-danger-free-elections#:~:text=A%20deepfake%20is%20a%20computer,to%20entertainment%2C%20hoaxes%20to%20harassment.

employee or agent thereof on a matter which is damaging to such other candidate or political party or employee or agent thereof; or

(2) willfully and knowingly participate in or conspire to participate in any plan, scheme, or design to violate paragraph (1).

(b) Fraudulent solicitation of funds

No person shall-

(1) fraudulently misrepresent the person as speaking, writing, or otherwise acting for or on behalf of any candidate or political party or employee or agent thereof for the purpose of soliciting contributions or donations; or

(2) willfully and knowingly participate in or conspire to participate in any plan, scheme, or design to violate paragraph (1).

The FEC has developed regulations governing the law against fraudulent misrepresentation at 11 C.F.R. §110.16. When the law and regulations against fraudulent misrepresentation are invoked, it is usually in reference to fundraising activities under the law [paragraph (b)]. The current petition for rulemaking is asking that the FEC clarify in its regulations that "deepfakes" are subject to the constraints specifically of paragraph (a) under the law in reference to campaign communications.

Deceptive deepfakes fit squarely into the parameters of 52 U.S.C. §30124. Specifically, by falsely putting words into another candidate's mouth, or showing the candidate taking action they did not, the deceptive deepfaker fraudulently speaks or act "for" that candidate in a way deliberately intended to damage him or her. This is precisely what the statute aims to proscribe. The key point is that the deceptive deepfake purports to show a candidate speaking or acting in a way they did not. The deceptive deepfake misrepresents the identity of the true speaker, which is an opposing candidate or campaign. The deepfaker misrepresents themselves as speaking for the deepfaked candidate. The deceptive deepfake is fraudulent because the deepfaked candidate in fact did not say or do what is depicted by the deepfake and because the deepfake aims to deceive the public. And this fraudulent misrepresentation aims to damage the campaign of the deepfaked candidate.

I. Applying the Goodman Test of Fraudulent Misrepresentation

A 2018 policy statement by former Republican Commissioner Lee Goodman provides a fairly narrow interpretation of the fraudulent misrepresentation statute and regulations. As noted above, the statute and regulations provide two separate prohibitions with respect to fraudulent misrepresentation. The first prohibits a candidate or the candidate's employees or agents from speaking or acting on behalf of another candidate or political party in a way that is deliberately damaging to the other candidate or political party. The second provision prohibits any person from misrepresenting themselves as speaking or acting on behalf of a candidate or political party for soliciting campaign contributions.

Paragraph (a) regulating campaign communications applies only to a candidate and the candidate's employees or agents and not to outside groups or other persons. This necessarily means that the law against fraudulent misrepresentation governing campaign communications, and any potential regulation that the FEC may promulgate, has limited reach. It is acknowledged that any proposed regulation addressing deepfakes in campaign communications at this point will not address abuses by outside groups. That would be a matter of broader legislation, which already has been introduced in Congress. Nevertheless, as observed above, many such abuses in the 2024 election cycle so far have come from

candidates and their agents, making such clarification that the regulations cover deepfakes by one candidate against another appropriate and necessary.

Goodman set out various factors to demonstrate fraudulent misrepresentation. Applying them to the case of deceptive deepfakes makes clear that deceptive deepfakes should properly be characterized as fraudulent misrepresentation.

1. A misrepresentation as to the identity of the speaker.

This factor practically defines what a deepfake is. A deepfake purports to show a candidate speaking or acting in a way they did not. The deepfake misrepresents the identity of the true speaker, which is an opposing candidate or campaign.

Deepfakes produced by artificial intelligence are categorically different than misstating what an opposing candidate believes and do not simply consist of painting or obfuscating actual events, images or statements of the target candidate, a point elaborated further below. Deepfakes are entirely fabricated by computer technology. The target candidate is in no way involved in the campaign communication and does not give consent to being cast in the misrepresentative messages. It is solely the deepfaking candidate who is creating the deceptive images and words of the deepfaked candidate.

2. No disclosure or countermanded disclosure.

Presumptively, Goodman contends, an adequate disclosure of who is issuing a campaign communication is sufficient to defeat a claim of fraudulent misrepresentation. That is because a disclosure will typically cure the confusion as to the identify of a speaker: A campaign leaflet from Candidate Jones stating that Candidate Smith believes the sun revolves around the earth does not confuse the voter about who is making the claim, and Candidate Smith is freely able to explain their true view. However, Goodman notes, an otherwise adequate disclosure can be countermanded when the misrepresentation in the text itself defeats the disclosure and perpetuates confusion about the actual speaker.

In the case of deceptive deepfakes, a disclosure of who is distributing the fraudulently misrepresented content will not cure the confusion about the actual speaker. If Candidate Jones places on their social media feed a deepfake video of Candidate Smith saying that the sun revolves around the earth, the disclosure that Jones is distributing the content does not cure the deception over identity. By contrast, a disclosure that the deepfake video is a deepfake would constitute an adequate disclosure, precisely because it would cure the confusion over identity.

3. Believability.

The notion of believability, Goodman argues, is necessary to show fraud: fraudulent misrepresentation requires that a reasonable person would perceive the deceptively false messages as being real. According to one federal court interpreting 52 U.S.C. §30124, a misrepresentation can be deemed fraudulent "if it was reasonably calculated to deceive persons of ordinary prudence and comprehension."[6]

[6] *FEC v. Vovacek*, 739 F. Supp. 2d (N.D. Texas April 14, 2010).

AI-generated deceptive deepfakes evidence an incredibly high standard of believability. Many deepfake images and audio clips are now indistinguishable from authentic content for the general public, even upon close inspection or listening – in other words, they certainly will deceive persons of ordinary prudence and comprehension. Deepfake video quality is slightly inferior, but already robust enough in cases where effort is made to deceive persons of ordinary prudence and comprehension. As the technology rapidly evolves, it is highly likely that, well before the 2024 elections, quality deepfake videos will be indistinguishable from authentic content for the general public, even upon close inspection.

4. Deceptive intent.

Finally, Goodman contends there must be deceptive intent. This will normally be inferred from the context of the case, he suggests.

With deceptive deepfakes, deceptive intent should be presumed. In fact, deception is the point of a deceptive deepfake: the entire purpose of generating such content is to deceive voters as to the identity of the speaker. One can imagine cases where the presumption could be rebutted, for example in the good faith forwarding of a deepfake where the party disseminating a deepfake did not generate the deepfake and genuinely did not know the deepfake was a deepfake, and had acted with reasonable care in disseminating it. However, absent special circumstances, deceptive intent can be easily inferred.

II. Deepfakes, Fraudulent Misrepresentation and Lying

The FEC's authority under 52 USC 30124 specifically addresses fraudulent misrepresentation, not lying or mischaracterization. Especially because the Supreme Court has held that lies are a form of constitutionally protected political speech (see below), it is important to clarify why deceptive deepfakes constitute fraudulent misrepresentation, as well as when deepfakes do not constitute fraudulent misrepresentation.

First, as elaborated in the discussion of the Goodman factors, the deceptive deepfake analysis is ***not*** about determining whether the deepfaking candidate lied about what their opponent's positions. The focus is on whether the deepfaking candidate deceptively spoke for their opponent – showing the target candidate saying or doing something that in fact they did not say or do.

Second, relatedly, the deceptive deepfake analysis does not require a fact-intensive review of the content. The prohibition is focused on the method or manner of speech. Creating or disseminating a deepfake that purports to show a candidate saying or doing something they did not, in a way designed to trick the voting public, is a fraud.

Third, as elaborated below in our discussion of First Amendment-related issues, this distinguishing of deepfakes from lies or mischaracterizations is necessary precisely because of one the key indicia of fraudulent misrepresentation: the ability of the targeted party to respond effectively. If a candidate misrepresents an opponent's position, the opponent can clarify the record. Voters can work out the truth for themselves. But if a candidate deepfakes another, the targeted candidate is not able to engage in effective counter-speech; the best they can do is deny the veracity of something that appears to authentic. In this circumstance, voters do not have the tools to find the truth for themselves.

Fourth, the prohibition on fraudulent misrepresentation would not apply in cases where there is a sufficiently prominent disclosure that the image, audio or video was generated by artificial intelligence and portrays fictitious statements and actions; the fact of a sufficiently prominent disclosure – a non-burdensome measure -- would eliminate the element of deception and fraud. This again distinguishes deceptive deepfakes from lies – for deepfakes, the cure does not require an alteration of the portrayed speech, but merely an adequate disclosure of who is actually speaking.

Fifth, the prohibition on fraudulent misrepresentation does not apply generally to the use of artificial intelligence in campaign communications, but only to deepfakes or similar communications. The fraud is not the use of AI technology, but the specific use of AI technology to defraud voters by deceiving them as to who is actually speaking or doing something. Similarly, the prohibition on fraudulent misrepresentation would not apply to cases of parody, where an opposing candidate is shown doing or saying something they did not, but where the purpose and effect is not to deceive voters and, therefore, where there is no fraud.

California and Washington prohibit deepfakes within a certain period of time before an election, unless the communication provides clear and concise disclosure that the deepfake is artificially generated.[7] They also provide exemptions for obvious satire or parody. These seem to be good models for regulations.

Public Citizen has proposed a model state law for regulating deepfakes that accommodates exceptions for clear and concise disclosure as well as obvious satire and parody. But such exceptions are not mandated under the law against fraudulent misrepresentation.

III. Deceptive Deepfakes and the First Amendment

Amending 11 C.F.R. § 110.16 to make clear that the prohibition on fraudulent misrepresentations extends to deceptive deepfakes would be consistent with the First Amendment. The government's power "to protect people against fraud … has always been recognized in this country and is firmly established." *Donaldson v. Read Magazine*, 333 U.S. 178, 190 (1948). And "[t]he state interest in preventing fraud … carries special weight during election campaigns when false statements, if credited, may have serious adverse consequences for the public at large." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 349 (1995); *cf. Burson v. Freeman*, 504 U.S. 191, 199 (1992) (recognizing that the government "has a compelling interest in ensuring that an individual's right to vote is not undermined by fraud in the election process").

Critically, 11 C.F.R. § 110.16, both as it exists now and as it would stand if amended, does not sweep in speech that may be constitutionally protected by targeting "false statements generally." *United States v. Alvarez*, 567 U.S. 709, 722 (2012) (plurality opinion). Rather, in targeting only *fraudulent* misrepresentations, the regulation covers only speech that falls outside the protection of the First Amendment altogether. *See Illinois ex rel. Madigan v. Telemarketing Assocs., Inc.*, 538 U.S. 600, 612 (2003) ("[T]he First Amendment does not shield fraud.").

[7] California Elections Code §20010; Washington Title 42 RCW.

Dispelling any doubt that the government can permissibly bar candidates and fundraisers from fraudulently misrepresenting their own identities, the Supreme Court has held that the government may constitutionally take the even stronger step of requiring speakers to affirmatively *disclose* the source of certain election-related communications. *See Citizens United v. FEC*, 558 U.S. 310, 367–71 (2010). As the Court explained, "transparency enables the electorate to make informed decisions and give proper weight to different speakers and messages." *Id.* at 371; *cf. First Nat'l Bank of Bos. v. Bellotti*, 435 U.S. 765, 792 n.32 (1978) ("Identification of the source of advertising may be required as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."). If requiring speakers to place disclaimers on their public-facing electoral communications can satisfy the "exacting scrutiny" that the First Amendment demands for compelled disclosures, *Citizens United*, 558 U.S. at 366 (quoting *Buckley v. Valeo*, 424 U.S. 1, 64 (plurality opinion)), then there is necessarily no constitutional problem with barring deliberate misrepresentations that are intended to induce detrimental reliance in the listener through deception and that are not covered by the First Amendment in the first place.

Moreover, in the context of campaigns for elected office, the government and the public have an especially strong interest in regulation prohibiting fraudulent misrepresentations that take the form of AI-generated deepfakes. When a candidate makes a deceptive verbal representation about an opponent, it is possible to mitigate the impact of the misrepresentation by persuasively exposing it as a lie. *See Alvarez*, 567 U.S. at 727 (plurality opinion) ("The remedy for speech that is false is speech that is true."). But deepfakes are attractive to fraudsters precisely because they are so impervious to counter-speech. When an impersonated candidate denies the veracity of a deepfake, the candidate does not simply challenge a third-party's competing claim; the targeted candidate can only offer a seemingly self-interested denial that the listener will have to judge against the strength of her trust in her own perceptions. The First Amendment does not shield fraud in any medium. It stands to reason, then, that the First Amendment surely does not shield fraud in a medium that is distinctly effective at defrauding.

Request for Rulemaking

In view of the novelty of AI generated deepfakes, and the speed with which the technology is improving, Public Citizen encourages 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 other candidates or political parties through deliberately false AI-generated content in campaign ads or other communications – absent clear and conspicuous disclosure in the communication itself that the content is generated by artificial intelligence and does not represent real events – then the restrictions and penalties of the law and the Code of Regulations are applicable.

Sincerely,

Robert Weissman
President, Public Citizen
1600 20th Street, N.W.
Washington, D.C. 20009
(202) 588-1000

Craig Holman, Ph.D.
Government affairs lobbyist, Public Citizen
215 Pennsylvania Ave., S.E.
Washington, D.C. 20003
(202) 454-5182