CENTER FOR DEMOCRACY & TECHNOLOGY

October 16, 2023

Federal Election Commission
Lisa J. Stevenson, Office of General Counsel
1050 First Street, NE
Washington, D.C. 20463

Submitted via the internet

Comments from the Center for Democracy & Technology on Public Citizen's Petition for Rulemaking on the use of Artificial Intelligence in Campaign Communications

Dear Ms. Stevenson:

On July 13, 2023, Public Citizen submitted a petition to the Federal Election Commission (FEC) to open a rulemaking process "to clarify that the law against 'Fraudulent Misrepresentation' (52 U.S.C. §30124) applies to deceptive AI campaign communications."[1] The Center for Democracy & Technology joins Public Citizen in calling for the FEC to open a rulemaking process to consider how it might limit fraudulent misrepresentations in election communications through the use of AI-generated media.

The use of artificial intelligence to produce synthetic video, images, or audio that has been digitally manipulated to misrepresent the voice and likeness of another person, or "deepfakes," is a growing reality in election campaigns.[2] As Public Citizen's petition notes, artificially produced fake audio of a Chicago mayoral candidate circulated on Twitter the day before the election, and in the Republican presidential primary, one candidate posted AI-generated fake images of another.[3] Similar examples come from abroad: at the end of September, a Slovak

[1] "Second Submission: Petition for Rulemaking to Clarify that the Law Against "Fraudulent Misrepresentation" (52 U.S.C. §30124) Applies to Deceptive AI Campaign Communications," Public Citizen (July 13, 2023).
[2] In 2023, the nonprofit research organization Freedom House found examples of AI to "sow doubt, smear opponents, or influence public debate" in "at least 16 countries." *See* Allie Funk, Adrian Shahbaz, and Kian Vesteinsson. "Freedom on the Net 2023: The Repressive Power of Artificial Intelligence."
[3] "AI-Generated Election Content Is Here, And The Social Networks Aren't Prepared," Irene Benedicto, *Forbes* (July 6, 2023); "DeSantis campaign shares apparent AI-generated fake images of Trump and Fauci," Shannon Bond, NPR (June 8, 2023).

political party posted a video containing voices imitating rival candidates to its YouTube and Facebook accounts. While text below the video said that any resemblance to other voices was "coincidental," a similar clip on WhatsApp portrayed one of the candidates as supporting an increase to the price of beer.[4] The month of this writing, synthetic audio of UK Labour Party Leader Keir Starmer making damaging comments appeared on the social media platform X during the Labour Party Conference in Liverpool.[5]

As generative AI tools become more readily accessible and easier to use, creation of convincing deepfakes will become faster and cheaper, and they are likely to proliferate.[6] Voice, in particular, can be spoofed quickly, cheaply, and easily: using just minutes of recorded speech, online services allow users to create convincing synthetic audio in moments for fractions of a cent per second. Satirical projects show that synthetic video and voice can be combined to produce hours of footage of candidates apparently saying things they never did in a debate that never happened.[7]

Although the FEC cannot alone solve the issues raised by the use of deepfakes in election campaigns, it can take a meaningful step forward by adopting rules that limit the ability of candidates to use AI-generated deepfakes to engage in fraudulent misrepresentations by putting words in the mouths of their opponents.

The FEC Has Authority to Act

Public Citizen's petition to the FEC points to 52 U.S.C. § 30124, which reads:

> *(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 employee or agent thereof on a matter which is damaging to such other candidate or political party or employee or agent thereof;*
>
> *(2) or willfully and knowingly participate in or conspire to participate in any plan, scheme, or design to violate paragraph (1).*

[4] "Progressive Slovakia becomes target of AI misinformation, tops polls," Barbara Zmušková, EURACTIV.sk (September 28, 2023).
[5] "Deepfake audio of Sir Keir Starmer released on first day of Labour conference," Sky News (October 9, 2023).
[6] "The People Onscreen Are Fake. The Disinformation Is Real," Adam Satariano and Paul Mozur, *New York Times* (February 7, 2023).
[7] "'Biden' vs. 'Trump' and the future of debate," Derek Robertson, *Politico* (June 21, 2023).

(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).

As part of its petition, Public Citizen included policy statements by three Republican Commissioners: one by former Commissioner Lee Goodman and a second issued jointly by current Vice Chair Allen Dickerson and Commissioner James "Trey" Trainor III. These opinions explain that the Commission has judged that fraudulent misrepresentation requires candidates to portray their speech as belonging to another. Goodman's policy statement is explicit: in cases of fraudulent misrepresentation in the solicitation of funds, "[t]he focus of the fraudulent misrepresentation inquiry must be the representation of *identity* of the person soliciting the funds, not the use to which the funds are put."[8]

The statements primarily base their arguments on 52 U.S.C. § 30124(b), which deals with fraudulent misrepresentation in the solicitation of funds. Under that statute, "[n]o person shall 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 solicitation contributions or donations." The thrust of the statutory language is clear: a person may not fraudulently misrepresent themselves as speaking or acting on behalf of a candidate or their agents when soliciting funds.

Public Citizen's petition is based on subsection (a) of the same statute, which addresses fraudulent misrepresentation in general, not limited to the fundraising context. Although subsection (a) reads slightly differently, the focus on misrepresentation of the identity of the true speaker is similar: "No person who is a candidate for Federal office or an employee or agent of such a candidate shall fraudulently misrepresent himself… as speaking or writing or otherwise acting for or on behalf of any other candidate or political party." This language provides clarity about what must be misrepresented in order for a message to violate 52 U.S.C. §30124(a): one candidate (or their agents) cannot misrepresent themselves as speaking for or on behalf of another candidate.

Deepfake technology makes exactly this type of misrepresentation possible. It provides the ability to take words composed by one candidate, the true speaker, and put them in the mouth of another. In other words, deepfakes provide a mechanism that allows a candidate to fraudulently misrepresent themself "as speaking or writing or otherwise acting for or on behalf of" another candidate by providing the ability to write and bring a script to life by appropriating

[8] Public Citizen 2023, p. 10. Italics in original.

that other candidate's voice and likeness. In past eras such a misrepresentation might be made by hiring an actor to fake recordings. This would be more difficult, time intensive, and prone to detection than the use of artificial intelligence. Like deepfake technology, such a scheme would defraud the public by misrepresenting both the true speaker and the candidate it falsely portrays. The more realistic the forgery, the less able the public is to attribute a message to its true speaker. This is the promise of the deepfake for political operatives.

Limits to the FEC's Authority Are Appropriate But Not Prohibitive

Both the First Amendment and the law as written place important limits on the Commission's authority under 52 U.S.C. § 30124. The FEC may not suppress satirical or other protected expression or set vague standards which chill permissible campaign speech. Most forms of content—even knowingly deceptive content, i.e. lies—are constitutionally protected.[9] Arbitrary rules governing common practices like placing candidate photos near quotations or accusatory text could chill significant amounts of First Amendment protected speech. Likewise, the use of photo-editing software to manipulate images of candidates is a widespread practice, which does not misrepresent the identity of a message's speaker or writer even if it may distort or be dishonest.

However, as Public Citizen's petition explains (at 6-7), the Supreme Court has made clear that the First Amendment does not protect fraudulent misrepresentations in the election process. Section 30124's emphasis on the fraudulent misrepresentation of a message's *origin* is consistent with this line: it sidesteps questions about a message's content entirely and focuses on misrepresentation of the message's speaker. Moreover, although courts often point to counter speech as a more limited and appropriate response than legislative or regulatory remedies,[10] counter speech is a poor remedy for misrepresentations embodied in deepfakes. When a candidate is targeted by a deepfake, any counter speech claiming fraud appears self-serving and is difficult to verify. Even technical experts have increasing difficulty telling high quality deepfakes apart from genuine artifacts; for the public at large it is a near hopeless task.

In addition to First Amendment limitations, the FEC has narrow statutory authority here. The law empowers it to regulate campaign finance and communications by candidates and their campaigns, but not by other important political actors during elections who play a larger role today than in the past. In addition, some common proposals, like outright bans on deceptive AI-generated content in campaign advertising—even if constitutional—would require legislation.[11]

---

[9] *See* *United States v. Alvarez*, 567 U.S. 709 (2012); *see also* *Susan B. Anthony List v. Driehaus*, 573 U.S. 149 (2014).

[10] *See* *Whitney v. California*, 274 U.S. 357 (1927).

[11] Legislation on these issues has been introduced at the federal level and has either been proposed or already passed in some states. *See, e.g.,* "Bipartisan push to ban deceptive AI-generated ads in US elections," Reuters (September 12, 2023); Cal. Elec. Code § 20010, "Campaign material with superimposed image of person prohibited," (accessed October 12, 2023); and Washington SB 5152 (accessed October 12, 2023). In Texas, a state bill would make "fabricating a deceptive video with intent to influence the outcome of an election" a criminal offense. *See* Texas S.B. 751 (accessed October 12, 2023).

Nevertheless, the FEC's statutory authority does permit it to engage in the narrow rulemaking sought here.

The FEC Should Consider a New Approach to Disclosures When Addressing Deepfakes

The FEC has long required disclosures about the source of election communications. FEC guidance to candidates and campaigns holds that "[a]ny public communication made by a political committee—including communications that do not expressly advocate the election or defeat of a clearly identified federal candidate or solicit a contribution—must display a disclaimer."[12] The Supreme Court has found these disclosure requirements to be consistent with the First Amendment: for instance in the 2003 case *McConnell v. FEC*, the Court found that the government interest in "shedding the light of publicity on campaign financing" is legitimate and strong enough for disclosure requirements to survive a First Amendment challenge.[13] More recently, the *McConnell* case was quoted in the 2010 *Citizens United v. FEC* decision, which held that disclosures do not impose undue burdens on political speech.[14]

The FEC also stipulates specific rules for disclosures on print, radio, phone, television, and internet communications (including email and websites). These disclosures variously require that the communication state who paid for it and which, if any, candidates or campaigns authorized the communication. It stipulates details on how these disclaimers should appear, for example by requiring a certain size of type on a color-contrasted background for print communications and an audio disclaimer accompanied by an image of a candidate "occupying no less than 80 percent of the vertical screen height" for television communications. Similar rules exist for text, audio, and video internet communications. This minutiae is important: it shows that communications not only must disclose their source, but do so in a way that is clear and accessible to the receiving audience.

The Commission has placed great importance on disclosures as an antidote to otherwise fraudulent misrepresentation. In nearly all but the most egregious of examples, messages attributed to other candidates in misleading or ambiguous ways can be protected from accusations of fraudulent misrepresentation if they include appropriate disclaimers of their true source. Conversely, a misleading disclosure falsely attributing a message to another candidate exposes the true speaker to allegations of fraudulent misrepresentation.

However, text and audio disclosures designed for previous forms of campaign advertising are inadequate for protecting the public from fraudulent misrepresentation through deepfakes. While past advertisements might make use of recorded audio from opposing candidates, in those cases the candidate did utter those words, regardless of whether or not they are quoted out of context. With deepfakes, however, the public would be unable to discern between "approved" messages containing genuine quotes from opponents and messages containing synthetic forgeries. Despite the disclosure of candidate approval for the overall advertisement or other

[12] "Advertising and disclaimers," Federal Elections Commission (accessed 10/12/2023).
[13] *McConnell v. Federal Elections Commission*, 540 U.S. 93 (2003)
[14] *Citizens United v. Federal Elections Commission*, 558 U.S. 310 (2010).

communication, the public would remain misled as to the true source of the words or actions falsely attributed to the opposing candidate in the deepfake, in effect allowing candidates to fraudulently misrepresent themselves as speaking on behalf of another.

As Commissioner Goodman's policy statement recognized:

> "A proper disclaimer clearly and accurately identifies the person responsible for the solicitation. Therefore, it affords a strong presumption against finding misrepresentation. That presumption *may nonetheless be defeated* where an explicit misrepresentation in the text of a solicitation countermands an otherwise accurate disclaimer.[15]

Synthetic audio or imagery appropriating a candidate's voice or likeness to portray actions never taken and words never said would constitute such an "explicit misrepresentation" sufficient to "countermand an otherwise accurate disclaimer." Hence, disclosure as to the source of the overall advertisement or communication is not sufficient to avoid misrepresentation as to the source of the words in the deepfake.

This technological moment thus requires consideration of new types of disclosures. The Commission should consider, for example, whether a message that the content of an advertisement contained AI-generated audio or imagery could mitigate the risk and harm of fraudulent misrepresentation. Some advertising platforms already require such disclosures.[16] As discussed above, 52 U.S.C. § 30124 provides the FEC with the authority to require both disclosures identifying a communication's true source, and, as an extension of that prerogative, the authority to require disclosure of AI-generated content in campaign communications.

The FEC should use the rulemaking process to determine the type(s) of disclosure that can mitigate the fraudulent misrepresentation otherwise resulting from a deepfake. For example, it should consider whether visual disclosures related to use of synthetic media be made continuously throughout video content (e.g., as a banner occupying a certain percentage of the image or as a watermark) and whether it should be accompanied by audio disclosures to reach visually impaired audiences.

The FEC might also clarify which uses of generative artificial intelligence do *not* require special disclosures, such as parodies or the use of artificial intelligence to simulate a candidate's *own* voice or appearance.

* * *

The consequences of allowing unrestrained deepfakes to proliferate in US elections could be dire. No healthy democracy can consistently elect leaders based on fraudulent misrepresentations. Moreover, public faith in the electoral process itself may be at stake: recent

[15] See Public Citizen 2023, p. 9. Italics added.

[16] "AI that alters voice and imagery in political ads will require disclosure on Google and YouTube," Michelle Chapman, AP (September 7, 2023).

polling shows that eighty-five percent of Americans are concerned about the spread of misleading video and audio deepfakes.[17] The Commission should open a rulemaking and act expeditiously to help protect our electoral process.

Respectfully submitted,

Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, DC, 20005

[17] "Majorities of Americans are concerned about the spread of AI deepfakes and propaganda," Taylor Orth and Carl Bialik, YouGov (September 12, 2023).