Dear Mr. Knop:

On behalf of The Leadership Conference on Civil and Human Rights (The Leadership Conference) and Common Cause, we write in response to the Federal Election Commission’s (FEC) above-referenced notice for comment regarding the Petition for Rulemaking (Petition) from Public Citizen.

The Leadership Conference, a coalition charged by its diverse membership of more than 240 national organizations to promote and protect the civil and human rights of all persons in the United States, works to ensure that technological innovation promotes equal opportunity for all—particularly for traditionally marginalized people and communities—inclusive democratic participation, privacy, and all forms of civil and human rights, and that these principles are at the center of communications and technology policy.

Common Cause is a nonpartisan, grassroots organization dedicated to upholding the core values of American democracy. We work to create an open, honest, accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

The FEC has a legislative mandate that provides it with tools that are well within the FEC’s authority to mitigate harms arising from artificial intelligence—deepfakes, in particular—which allows certain steps that can provide some protection for the integrity of our elections. The Petition asks the FEC to amend its regulation on “fraudulent misrepresentation,” 12 at 11 C.F.R. 110.16, to clarify that “the restrictions and penalties of the law and the Code of Regulations are applicable” should “candidates or their agents fraudulently misrepresent other candidates or political parties through deliberately false Artificial Intelligence-generated content in campaign ads or other communications.” As evolving technology presents new challenges, federal agencies must ensure that all applicable regulations are updated and relevant. Our organizations agree that amending the regulation is vitally necessary to ensure that the regulations keep pace with new technology that could enable novel forms of fraudulent representation. An informed and engaged public, which is a requisite for a well-functioning democracy, is a core element of election integrity.
I. AI Use in Elections Today

Academics and researchers have been sounding the alarm about the use of deepfakes in our elections since well before the dramatic rise in interest in AI among policymakers this year. In 2019, both the Senate and House of Representatives held hearings on the challenges of deepfake technology, where experts educated lawmakers about potential risks to democracy and national security stemming from malicious use of the technology.\(^1\) The general public is also beginning to understand the risk posed by the use of AI in our elections, with surveys showing anywhere from 70 percent to 85 percent of people concerned about the role AI deepfakes and other AI-generated content could play in the spread of misinformation.\(^2\) At the same time, research is raising concerns about the ability of viewers to recognize deepfakes when they see them. For example, a study by the Rand Corporation found that 27 percent to 50 percent of respondents were unable to distinguish deepfakes related to climate change; adults and educators, disturbingly, were the most vulnerable to being fooled by deepfakes.\(^3\)

There have been several recent examples of the use of deepfakes and other AI generated content in federal, state, and local elections. For example, the Petition cites the misuse of AI technology in the 2023 Chicago mayoral election and by Florida Governor Ron DeSantis’ presidential campaign.\(^4\) Other examples include the Republican National Committee’s use of AI in April to produce a video warning about potential dystopian crises during a second Biden term,\(^5\) and a deepfake circulated depicting Sen. Elizabeth Warren, D. Mass., insisting that Republicans should be barred from voting in 2024.\(^6\)

The availability of generative AI tools makes it easier than ever to increase the ability to spread false information and propaganda, as well as its scale, leaving voters confused and further questioning what they see and hear. Past disinformation campaigns created fake accounts on social media sites, developed fake media, and amplified and spread false information.\(^7\) AI systems give them another powerful and

---

6. Id.
destructive tool in the toolbox, and candidates and political parties will certainly take advantage of these tools if the FEC permits them to.

Meanwhile, political campaigns and candidates looking for possible legal remedies have extremely limited options in the face of the deep concern about the potential dangers they have expressed. The current lack of federal regulation contributes to creating a high degree of uncertainty going into the 2024 presidential election. Simply put, there is a compelling need for the FEC to take action and provide clarity using its existing authority.

II. Harms to Democracy

AI deepfakes and other AI-generated content have the potential to dramatically boost election disinformation and threaten the integrity of our elections, to the detriment of every person and political party. The decline in local news has meant that more Americans look to social media as their primary source of information. The risk is significantly increased because social media companies have continued to abdicate their responsibility to protect their users from disinformation and have reduced or even decimated teams dedicated to information integrity. Simply put, Americans are inundated with lies and manipulative content from both domestic and foreign actors and, as a result, are losing faith in our democracy.

Our nation has witnessed a precipitous growth in election disinformation since 2016, and over the same time, has experienced a decline in public trust in our elections and their results. Americans trust fewer and fewer news sources. In this online environment, AI deepfakes can only supercharge disinformation and increase distrust online.

As stated above, AI deepfakes are already appearing in our elections and as we get closer to the 2024 election, it is certain that this practice will proliferate without intervention from the FEC. In this information ecosystem, there are fewer trustworthy sources every day. There is nothing more important to a functioning democracy than an informed public, and without trustworthy news sources, voters will not have the information they need to participate in our democratic process.

---

The Petition for rulemaking describes precisely how it is within the FEC’s authority to act. It covers only information that is purported to be from a federal candidate or political party or their agents and employees. In this increasingly complex information ecosystem, it is critical that citizens know that the images, videos, and other media that they view in a campaign ad from a candidate for public office are authentic. In the world’s oldest continuous democracy, an individual running for public office should have a higher bar for authenticity and integrity than the thousands of disinformation-spewing troll accounts on social media.

III. Harms to Vulnerable Communities

Black, Latino, AAPI, and other communities of color have historically been targets of voter suppression and disinformation campaigns. These campaigns have been orchestrated by both outside groups, and by official campaigns themselves. This will not change with the ever-increasing use of generative AI. Over the past six years, online trolls have frequently impersonated Black users online -- attempting to sow distrust and suppress turnout. Other bad actors have also taken advantage of the limited resources social media platforms devote to addressing disinformation targeted at the Latino and AAPI communities to spread disinformation and create doubt in our political institutions. People with disabilities also have to deal with the consequences that stem from misinformation and the voter suppression campaigns that are often driven by false information. Generative AI now gives bad actors and political campaigns more ability to commit these practices, with increasing precision and realism. In addition, concerns about the biases in deepfake-detection software mean that the systems used to identify deepfakes may not, for example, be able to recognize darker skin tones. This makes the need for the FEC to regulate deliberately deceptive AI-produced content in campaign communications all the more pressing.

---

Non-English speakers are also particularly vulnerable to fraudulent campaign communications, and many AI-detection tools also struggle with content that contains languages other than English. Social media platforms are less likely to enforce their policies against disinformation and misinformation with respect to non-English content, with one study finding that non-English disinformation is left up 70 percent of the time, as compared to 29 percent of the time for English disinformation. This gap in enforcement presents an opportunity for bad actors to exploit. The FEC can help to ensure that campaigns do not target these communities with fraudulent AI-generated content.

IV. Legal Basis for Amending FEC Regulation

We recognize that AI deepfakes are a new technology and that questions about whether their use and abuse are captured under existing statutes are still being debated. The FEC has both the responsibility and the authority to provide the necessary clarity and make it clear that AI deepfakes are subject to the Federal Election Campaign Act’s prohibitions on fraudulent misrepresentation.

52 U.S.C. §30124 prohibits candidates from “fraudulently misrepresenting” themselves as acting on behalf of another candidate or party in a way that damages that candidate or party. By definition, deepfakes are fraudulent misrepresentations as they can be created without the notice or consent of the subject. AI deepfakes misrepresent the actual speaker and appear to be the person who is the subject of the deepfake, when actually the speaker could be the opposing candidate or party, the creator of the deepfake. Ads that use AI deepfakes will not only damage opposing candidates or parties but also the democratic process itself by creating media that depicts candidates saying things they have never said or doing things they have never done. This goes to the essence of what the statute is trying to prevent.

We agree with the Petition that this would not apply in scenarios of: i) parody where the attempt is not to deceive viewers: ii) where forms of AI technologies are used other than deepfakes: and iii) when there is a prominent disclaimer that makes it apparent to a reasonable person that AI deepfakes were used.

Congress has recognized the threat concerning deepfakes as well. The National Defense Authorization Act for Fiscal Year 2020 requires the Director of National Intelligence to submit a report on the threat of deepfakes used by foreign governments “to spread disinformation or engage in other malign activities.” The law also recognizes that AI deepfakes could be used in political contexts and requires the Director of National Intelligence to assess how deepfakes could harm the United States with respect to “the attempted discrediting of political opponents or disfavored populations.” Similarly, the IOGAN Act instructs the


National Science Foundation to fund research into generative adversarial networks—the underlying technology for AI deepfakes—calling for more research on “best practices for educating the public to discern authenticity of digital content.” These laws recognize the ability for AI deepfakes to be used in fraudulent ways and aim to align the federal government to be able to counter their threat.

V. Examples of State Laws

States have also moved to counter deepfakes with several laws to stop AI deepfakes, and many more such bills are moving through state legislatures.

For example, California Elections Code - ELEC § 20010 prohibits the malicious distribution of “materially deceptive audio or visual media” with the intent to deceive voters or injure a candidate’s reputation. The law creates a safe harbor for content that explicitly carries a disclosure describing the image or video to be “manipulated.” This aligns with the Petition, where a disclaimer would ensure the political ad does not qualify as a “fraudulent misrepresentation.”

Similarly, Texas Election Code 15 § 255.004 prohibits the creation and distribution of a deepfake video intended to “injure a candidate or influence the result of an election” within 30 days of an election. The bill specifies that the video must depict an “action that did not occur in reality,” again aligning with the exemptions specified in the Petition that stipulate it would only be a violation of the federal code if the AI deepfake depicts false incidents or speech.

As states make inroads on this issue, it is important that the FEC not be sidelined in upholding its responsibilities.

VI. Conclusion

In recent months, there has been an explosion in interest in regulating AI, from regulatory agencies to Congress to state and local governments. AI deepfakes are the next dangerous frontier of disinformation, and they are particularly easy to create and disseminate. If unregulated, these ads will harm candidates and deceive voters. Further, they have the potential to accelerate the ongoing erosion of trust in our democratic systems. The FEC not only has the authority, but the duty, to step in and protect voters and our democracy from lies, deception, and fraud.

The Petition represents a common-sense proposal, and it would have a meaningful impact on federal elections in 2024 and beyond by promoting transparency and holding individuals running for public office to a higher standard. We encourage the FEC to issue regulations that clarify that AI deepfakes used to deceive voters are “fraudulent misrepresentation” and enforce those regulations against parties that violate them.

Thank you for your consideration of our views. If you have any questions about this comment, please contact Jonathan Walter, policy counsel for media/tech at The Leadership Conference on Civil and Human Rights, at walter@civilrights.org, or Ishan Mehta, Director for Media and Democracy, Common Cause, at imehta@commoncause.org.
Sincerely,

Jesselyn McCurdy
Executive Vice President for Government Affairs
The Leadership Conference on Civil and Human Rights

Ishan Mehta
Director for Media and Democracy
Common Cause
Washington DC