

Federal Election Commission
1050 First Street, NE
Washington, DC 20463

Re: Artificial Intelligence used for fraudulent election behavior

Dear Chair Lindenbaum, Vice Chairman Cooksey, and Commissioners Broussard, Dickerson, Trainor III, and Weintraub:

By notice published August 16, 2023, the Federal Election Commission has requested comments in response to a petition for rulemaking from Public Citizen calling on the Commission to clarify that AI-generated fraudulent misrepresentations should be treated as any other fraudulent misrepresentations would.¹ The Electronic Privacy Information Center (“EPIC”) strongly supports Public Citizen’s Petition (“Petition”) and believes that granting the Petition is the absolute minimum action the FEC should take to protect voters and election integrity from the proliferation of AI ahead of the 2024 elections.

EPIC is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC conducts research and advocates for common sense regulation concerning automated decision-making systems, including through our recent report describing how generative AI (“GAI”) will exacerbate misinformation and disinformation in elections and other contexts.²

GAI threatens to supercharge the current problem of misinformation and disinformation by making it bigger, faster, and more convincing. Although the Commission notes the Petition’s view that the “technology is not so far advanced currently that viewers are unable to identify when it is used disingenuously,”³ research underscores the urgency of FEC action ahead of the 2024 election. A 2021 study found that the average person cannot reliably detect deepfakes, that awareness doesn’t improve detection, and that voters believe deepfakes to be authentic more often than they believe authentic information is a deepfake—despite voters’ confidence in their ability to discern between the two.⁴

¹ Artificial Intelligence in Campaign Ads, 88 Fed. Reg. 55,606 (Aug. 16, 2023), <https://www.govinfo.gov/content/pkg/FR-2023-08-16/pdf/2023-17547.pdf>.

² Calli Schroeder, Ben Winters, et. al, *Generating Harms: Generative AI’s Impact & Paths Forward*, EPIC (May 2023), <https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf>.

³ *Supra* note 1 at 55,606.

⁴ Nils C. Kobis, Barbora Dolezalova, & Ivan Soraperra, *Foiled twice: People cannot detect deepfakes but think they can*, 24 *iScience* 1 (2021), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8602050/>; Pranshu Verma and Will Oremus, *AI Voice clones mimic politicians and celebrities, reshaping reality*, The Washington Post (Oct. 15, 2023), available at <https://www.washingtonpost.com/technology/2023/10/13/ai-voice-cloning-deepfakes/>.

The FEC should clarify in its regulations what is already clear in fact: fraudulent misrepresentation includes “candidates or their agents fraudulently misrepresent[ing] other candidates or political parties through deliberately false [Artificial Intelligence]-generated content in campaign ads or other communications.”⁵ This is an essential piece of the puzzle when it comes to stemming the information manipulation that GAI threatens to turbocharge.

For example, the following GAI products—based on models like Llama, GPT-4, and others—could be used to intentionally make fake text, videos, and voice messages:

- ❑ Conversational chatbots like ChatGPT, Bing Chat, Google Bard, Jasper Chat, and Hugging Chat;⁶
- ❑ Writing assistants like Jasper, Compose AI, Rytr, Copy.ai, and Lavendar;⁷
- ❑ Text-to-image generators like Bing Image Creator, DreamStudio, Craiyon, and MidJourney;⁸
- ❑ Image editors like PhotoRoom, GAI integrated into Adobe Photoshop, Luminar Neo, and Auto Enhance, as well as design tools like Brandmark;⁹
- ❑ Video generators like Syntheseia, Hour One, Lumen5, Pictory, and Elai;¹⁰
- ❑ Video editors like Descript and InVideo;¹¹ and
- ❑ Speech generation tools like PolyAI, Podcast.AI, and Descript Overdub.¹²

These tools, combined with the ease of accessing contact information of targeted groups through data brokers and the wide swath of available robocalling products, present a clear danger to the integrity of elections. This concern is not speculative. We have already seen examples of AI-facilitated fraudulent misrepresentations by campaigns and affiliated third parties, including:

- ❑ A falsified video of Governor Ron DeSantis withdrawing from the race for the Republican presidential nomination spread rapidly online, using his face and voice to create a deepfake;¹³
- ❑ Former President Trump shared a deepfake video of CNN anchor Anderson Cooper saying that Donald Trump “ripped them a new asshole” at the end of the a town hall, which is not what Cooper said.¹⁴

⁵ Petition at 5.

⁶ Ben Winters & Bijal Mehta, *The Many Forms of GAI*, EPIC (Sept. 7, 2023), <https://epic.org/the-many-forms-of-generative-ai/>.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ Peter Suclu, *There is Now a Deep Fake Video of Ron Desantis Dropping Out of the 2024 Race*, Forbes (Sept 2, 2023) <https://www.forbes.com/sites/petersuciu/2023/09/02/there-is-now-a-deep-fake-video-of-ron-desantis-dropping-out-of-the-2024-race/?sh=5ddc05187bf9>.

¹⁴ Alexandra Ulmer & Anna Tong, *Deepfaking it: America's 2024 election collides with AI boom*, Reuters (May 30, 2023), <https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/>.

- Earlier this year, Indian lawmaker Palanivel Thiagarajan was able to create doubt about genuine audio clips from his speech by claiming that the audio was AI generated.¹⁵ By showing that AI is capable of generating convincing false audio, Thiagarajan cast enough doubt about the origin of the clips to avoid accountability for the content of what he said.
- In Slovenia, “[v]ideos featuring AI-generated deepfake voices of politicians [spread] on social media ahead of the Slovak parliamentary elections ... including a two-minute-long conversation in which the leader of the progressive party, Michal Simecka, appears to discuss buying votes from the Roma minority with a journalist.”¹⁶

Advocacy groups are not alone in recognizing the threat. The Department of Homeland Security echoed these same concerns in its 2024 Homeland Threat Assessment:

GAI enables the rapid creation of an endless supply of higher quality, more idiomatically correct text, providing influence actors the ability to expand their messaging and give it a greater aura of credibility. Already, hundreds of websites have used a publicly available, large-language, model-based chatbot to generate content, some of which was false or misleading. For example, in April, a Chinese government-controlled news site using a GAI platform pushed a previously circulated false claim that the United States was running a lab in Kazakhstan to create biological weapons for use against China. Recently, Russian influence actors have used new AI technology in select cases to augment their operations. For instance, in June, an RT (formerly Russia Today) social media account created and shared a deepfake AI-generated video disparaging the US President and other Western leaders.¹⁷

The Election Administration Commission has also explained that “[o]ne key weakness of AI chatbots is that these systems create false information, sometimes called “hallucinations.” These tools can produce inaccurate or misleading content, even when they provide sources for their responses. Any text generated with an AI chatbot should be thoroughly reviewed for accuracy.”¹⁸

EPIC urges the FEC to act swiftly in initiating this rulemaking and is eager to discuss how the FEC can mitigate the negative effects of disinformation facilitated and exacerbated by generative AI. Please don’t hesitate to reach out to EPIC Senior Counsel Ben Winters at winters@epic.org or 202-483-1140 x 126.

¹⁵ Niles Christopher, *An Indian politician says scandalous audio clips are AI deepfakes. We had them tested*, Rest of World (July 5, 2023), <https://restofworld.org/2023/indian-politician-leaked-audio-ai-deepfake/>.

¹⁶ Olivia Solon, *Trolls in Slovakian Election Tap AI Deepfakes to Spread Disinfo*, Bloomberg (Sept. 29, 2023), <https://www.bloomberg.com/news/articles/2023-09-29/trolls-in-slovakian-election-tap-ai-deepfakes-to-spread-disinfo>.

¹⁷ Dep’t of Homeland Sec., *2024 Homeland Threat Assessment* 6 (Sept. 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf.

¹⁸ Election Assistance Comm’n, *AI Toolkit for Election Officials* (Aug. 2023), https://www.eac.gov/sites/default/files/2023-08/AI_Toolkit_Final_508.pdf.

Sincerely,

/s/ Ben Winters

Ben Winters

Senior Counsel

Electronic Privacy Information Center