FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

October 16, 2023

Via Electronic Submission
Federal Election Commission
Attn: Lisa J. Stevenson
1050 First Street, NE
Washington, DC 20463

Re: REG 2023-02 Artificial Intelligence in Campaign Ads

Dear Ms. Stevenson,

The Future of Privacy Forum (FPF) supports the Petition urging the Federal Election Commission (the "Commission" or "FEC") to begin a rulemaking to amend its regulation on "fraudulent misrepresentation" of campaign authority to make clear that the statutory prohibition applies to deliberately deceptive artificial intelligence (AI)-generated campaign ads.[1] As AI technology becomes even more advanced, it will be critical to proactively implement regulations on the proper use of AI and, more specifically, generative AI to create or distribute election-related content.

FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally.[2] We seek to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective rules.

In August 2023, FPF's Vice President of U.S. Policy Amie Stepanovich, and Policy Counsel Amber Ezzell published an op-ed in *The Hill*, "Generative AI could be used to steal the next election and how we can stop it."[3] The article highlights the potential for generative AI to manipulate voters and election outcomes, while also illustrating benefits reaped for voters and candidates when generative AI tools are deployed ethically and responsibly:

> *The potential political uses of generative AI are endless. Candidates and parties may use it to help write prime-time national advertisements as well as micro-targeted text messages tailored to specific voters. Meanwhile,*

---

[1] Artificial Intelligence in Campaign Ads, 88 Fed. Reg. 55,607 (Aug. 16, 2023) (to be codified at 11 C.F.R. pt. 112), https://sers.fec.gov/fosers/showpdf.htm?docid=423639; 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), https://sers.fec.gov/fosers/showpdf.htm?docid=423502; *See also* 52 U.S.C. § 30124; 11 C.F.R. § 110.16.

[2] The views expressed in this comment are those of FPF and do not necessarily represent the opinions of our Advisory Board.

[3] Amie Stepanovich and Amber Ezzell, *Generative AI could be used to steal the next election and how we can stop it*, The Hill (Aug. 3, 2023), https://thehill.com/opinion/campaign/4133062-generative-ai-could-be-used-to-steal-the-next-election-here's-how-we-can-stop-it/

> *the next generation of political memes set to dominate certain corners of social media may very well be AI-driven. No longer must a candidate's supporters rely on their own photo editing skills to create political images; they can provide prompts to online generative AI tools that will create the images for them.*

The FEC is well-suited to initiate a rulemaking to clarify how "fraudulent misrepresentation" applies to deliberately deceptive AI-generated campaign ads. Such a rulemaking presents an opportunity to protect the integrity of elections and campaigns, as well as to preserve and increase public trust in the growing uses of AI by candidates and in campaigns. While public trust in the election process is critical to democracy, generative AI carries the potential to erode public trust and damage the integrity of campaigns, elections, and campaign communications. The use of deceptive design in elections poses a risk for the spread of misinformation, voter suppression, and harassment of candidates – especially for marginalized individuals.[4]

When generative AI is used carefully and responsibly, it can be used to reach different segments of the population and facilitate the creation of campaign ads that address the needs and concerns of specific groups and populations. We urge the Commission to further use this rulemaking opportunity to investigate the need for and potential of risk mitigation, planning, education, and outreach for populations most at risk, to ensure that AI does not become another vector for the spread of misinformation and voter suppression.

We have attached the op-ed in *The Hill* as an addendum to this submission, and also welcome any further opportunity to provide resources or information to assist in the Commission's effort to strengthen its regulation in the midst of rapid developments in technology, particularly regarding AI. If you have any questions about the op-ed or FPF's work in the area of generative AI, please contact FPF Policy Counsel Amber Ezzell.

Thank you,

Amber Ezzell
Policy Counsel, Future of Privacy Forum
aezzell@fpf.org

[4] *See* Erin Spencer Sairam, *Women in Politics Have to Deal with More Harassment and Violence. A New Database Tracks the Threats*, Forbes (Nov. 2, 2022), https://www.forbes.com/sites/erinspencer1/2022/11/02/women-in-politics-have-to-deal-with-more-harassment-and-violence-a-new-database-is-tracking-those-threats/.

ATTACHMENT:

"Generative AI could be used to steal the next election and how we can stop it," an op-ed published in *The Hill* on August 3, 2023 by FPF Vice President of U.S. Policy Amie Stepanovich and FPF Policy Counsel Amber Ezzell

Attached to FPF's Submission to the Federal Election Commission Notice of Availability of Petition for Rulemaking on Artificial Intelligence in Campaign Ads

Generative AI could be used to steal the next election — here's how we can stop it

Amie Stepanovich and Amber Ezzell, Opinion Contributors

"I don't invite her to events," says former President Donald Trump about Iowa Gov. Kim Reynolds in a new campaign ad from presidential rival Ron DeSantis.

Except Trump never spoke those words at all — the voice was generated through artificial intelligence (AI) technology, and is maybe the first major example of what may become the next frontier of political campaign tools and tactics in the 2024 elections and beyond.

While generative AI can be used for good in elections, including to inform and educate voters, it can also be misused to spread misinformation, suppress voter turnout and harass candidates. We must invest now in risk-mitigation planning, education and outreach tools, particularly for our most at-risk populations.

Generative AI algorithms can be used to generate text, audio, images, videos, computer code or other content. Today, students are using generative AI to conduct research, designers use AI tools to create graphic and video ads and AI-powered voices are narrating audiobooks. Some applications are promising, but AI also poses risks to election integrity and individuals' safety on a scale not seen before. These threats require a coordinated response.

The potential political uses of generative AI are endless. Candidates and parties may use it to help write prime-time national advertisements as well as micro-targeted text messages tailored to specific voters. Meanwhile, the next generation of political memes set to dominate certain corners of social media may very well be AI-driven. No longer must a candidate's supporters rely on their own photo editing skills to create political images; they can provide prompts to online generative AI tools that will create the images for them.

In fact, before the ad with Donald Trump ever surfaced, Gov. DeSantis's PAC used generative AI to alter an image of him at a campaign rally to include fighter jets. The authenticity of photos and videos is becoming difficult to prove. When generative AI tools can be leveraged to hoodwink voters, candidates will need to discredit increasingly convincing records of things they never did or said.

The United States doesn't have a law to govern the use of generative AI for electioneering — although general election laws would still apply — and political campaigns are exempt from many state privacy laws. There is little mandated transparency into how political organizations or campaigns gather or use data, and none for unaffiliated supporters or unofficial groups that tend to produce the most

radical content.

The Terms of Use for generative AI engines vary widely. Some organizations prohibit the use of their tools for political content (though a determined user is likely to find workarounds), while others have more specific, if limited, prohibitions on deceptive impersonation or harassment. These also may offer little shield, since detection and enforcement is not likely to happen before a great amount of content is generated and stored.

While generative AI may have many uses in elections to persuade, influence or even mislead, its most nefarious uses may be to amplify pre-existing discrimination and inequitable practices. Generative AI can be a force multiplier for hateful messages, images, anecdotes or rumors; voters and candidates from historically marginalized communities will likely be disproportionately affected. While many candidates today are familiar with abuse and harassment, women in politics receive threats approximately 3.4 times more frequently than men. Those numbers are likely much higher for women of color and other marginalized groups.

Even when harassment is not the aim, bias may still permeate the use of generative AI. For instance, feminine users of AI-powered image generators have found they are more likely to receive outputs that are sexually suggestive. This shrouded but pervasive discrimination can be even more harmful because it hides the bias embedded in society's history beneath a veneer of a theoretically neutral algorithm.

Voters are also at risk for manipulation through messaging created with generative AI, where anyone can write in a voice that is tailored for specific communities. The potential for misleading election news to spread is greater with individuals who are not fluent English speakers, given English is the exclusive language for most educational materials and resources designed to detect and counter misinformation.

The credible claims of Russian interference in the 2016 U.S presidential election led to a heightened investment in tools to secure our election infrastructure and monitor all systems for suspicious behavior. The result was what has been called "the most secure election in U.S. history" in 2020 — not for lack of attempts to compromise it, but for resources to combat those attempts. In advance of the 2024 presidential election, we will need a similarly coordinated effort to prepare for the impacts of generative AI and other technological advancements.

To start, we must encourage active conversations with stakeholders from all sectors, demographics, backgrounds and areas of expertise, to provide guidance for how generative AI could be lawfully and ethically incorporated into organizations.

We must also remain vigilant. History has taught us how messaging can be used to radicalize individuals, and how to mitigate these risks. Consider the power of basic education in the labeling of

nutrition facts, advertising and for hazardous products. It's as crucial to invest in long-term digital literacy as short-term response.

There is genuine potential for generative AI to have a positive and lasting impact on human society. We must commit to ensuring that it is deployed ethically, with respect for the people it affects and alongside sufficient resources to identify and respond when and how it may be misused.

Amie Stepanovich is an internationally recognized expert in domestic surveillance, cybersecurity and privacy law. She is currently vice president for U.S. policy at the Future of Privacy Forum.

Amber Ezzell is a policy counsel at the Future of Privacy Forum. Her work focuses on a variety of consumer and commercial privacy matters, from technology-specific areas to general data management and privacy issues.