FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Disclosure and Transparency of	)	MB Docket No. 24-211
Artificial Intelligence-Generated	)	
Content in Political Advertisements	)	

Relating to the
Notice of Proposed Rulemaking
Issued August 5, 2024

Comments of the

Electronic Privacy Information Center

September 4, 2024

By:
Grant Fergusson
Counsel
fergusson@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

COMMENTS

I. Introduction

The **Electronic Privacy Information Center (EPIC)**[1] files these reply comments on the Federal Communications Commission's (FCC's or the Commission's) Notice of Proposed Rulemaking (NPRM) regarding "Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements," issued on August 5, 2024.[2] We applaud the Commission's efforts to safeguard the public from the harms of false, misleading, and deceptive AI-generated political content. However, we fear that, without additional provisions, the Commission's proposed disclosure and transparency rules will be ineffective at mitigating the harmful effects of using AI-generated content in political ads. Our recommendations herein reflect the Commission's interest in ensuring that the public has the necessary information to meaningfully evaluate political ads while emphasizing the use cases and features of AI-generated content that undermine public trust in and evaluation of political communications.

EPIC broadly supports the Commission's efforts to increase transparency and accountability over the use of AI-generated content in political ads. Broadcasters play a crucial role in informing the public of matters relevant to the American democratic process, but convincing AI deepfakes and other false, misleading, or otherwise deceptive AI-generated content threaten to undermine both broadcasters' legitimacy and the American political process writ large.[3] It is within both the Commission's authority[4] and the public interest to implement some form of transparency and accountability requirements for AI-generated content in political ads.

Transparency and accountability over AI-generated content is necessary to ensure that AI systems are not used to obscure, mischaracterize, or fabricate important political information. As

[1] The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC has filed several comments with the FCC regarding privacy and consumer safety, *see, e.g.*, Comments of EPIC, *In re* Location-Based Routing for Wireless 911 Calls, PS Dkt. No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009, and with various federal agencies on AI risks and harms, *see, e.g.*, EPIC, Comments on the Draft Documents Responsive to NIST's Assignments Under Executive Order 14110 (Sections 4.1, 4.5, and 11) (June 2, 2024), https://epic.org/wp-content/uploads/2024/06/EPIC-Comment-NIST-GenAI-Draft-Documents-06.02.24_Appendices.pdf.

[2] Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements, Proposed Rule, 89 Fed. Reg. 63,381 (Aug. 5, 2024), https://www.federalregister.gov/documents/2024/08/05/2024-16977/disclosure-and-transparency-of-artificial-intelligence-generated-content-in-political-advertisements.

[3] *See* EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* 1–8 (2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf (discussing use of AI-generated content to mislead or manipulate) [hereinafter "Generating Harms I Report"]; EPIC, *Generating Harms II: Generative AI's New & Continued Impacts* 1–8 (2024), https://epic.org/wp-content/uploads/2024/05/EPIC-Generative-AI-II-Report-May2024-1.pdf (discussing use of AI-generated content to influence elections) [hereinafter "Generating Harms II Report"].

[4] *See* Communications Act of 1934, 47 U.S.C. § 317; 47 C.F.R. § 73.1212.

the World Economic Forum noted in January of this year, AI-generated misinformation and disinformation are some of the most severe global risks of our time, stoking political polarization and undermining both electoral processes and the foundations of trust in communications infrastructure.[5] Without transparency into how and when AI systems are used for political messaging—transparency that must flow from AI developers and content producers to broadcasters, listeners, and viewers—we cannot pursue the "First Amendment's goal of an informed electorate that is able to evaluate the validity of messages and hold accountable the interests that disseminate political advocacy."[6]

However, meaningful transparency over the role of AI-generated content in political advertising will require more than the vague on-air announcements proposed by the Commission. Without (1) procedures for clarifying what aspects of political ads are AI-generated, (2) techniques for verifying the existence of AI content, and (3) restraints on the most harmful and distortive broadcasts of AI-generated political content, any public disclosure regime for AI-generated content within political ads will fall short of serving the public interest. To ensure the Commission's proposed rules are maximally effective at serving the public interest and mitigating harms, the Commission should increase the specificity of required on-air AI announcements such that listeners and viewers can accurately discern what aspects of an ad are AI-generated. To further increase transparency over AI-generated content in political ads, we also urge the Commission to require broadcasters to inquire into—and then include as part of their online political files—the existence of any AI watermarks, whether in audio, visual, or other format, within political ads that have AI-generated content. And beyond any proposed public disclosure rules, we urge the Commission to reconsider implementing limited restraints on the most harmful uses and broadcasts of AI-generated political content.

II. Vague Disclosures About Political Ads Containing AI-Generated Content Risk Blurring the Distinction between Truthful and False Content

Although EPIC broadly supports the Commission's proposed inquiry and disclosure rules for AI-generated content in political ads, we urge the Commission to increase the specificity of broadcasters' on-air announcements to explain what *aspects* of a political ad are created, altered, or otherwise influenced by an AI system. The ability of a listener or viewer to understand and evaluate AI-facilitated political ads depends not on their understanding that a political ad used AI-generated content in *some* capacity, but on their ability to discern what elements of a political ad are AI-generated. There is a world of difference between the political impact of AI-generated jingles and AI deepfakes of opposing political candidates, yet the Commission's proposed rule

[5] World Econ. Forum, Marsh McLennan, & Zurich Insurance Group, *The Global Risks Report 2024* 7–8 (2024), https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf; *Generating Harms II Report* at 2–4.

[6] *Standardized and Enhanced Disclosure Requirements for Television Broadcast Licensee Public Interest Obligations*, Second Report and Order, 27 FCC Rcd 4535, 4543–44, para. 16.

requiring broadcasters to make on-air announcements would not differentiate between disparate AI use cases.

The public risks of AI-generated content in political ads stem not only from advertisers' ability to convincingly present AI-generated content as real, but also from their ability to convincingly present real content as AI-generated—a concept that legal scholars Robert Chesney and Danielle Citron coin the "Liar's Dividend."[7] The Liar's Dividend raises two issues with the Commission's proposed approach. First, as Chesney and Citron note, a "person accused of having said or done something might create doubt about the accusation by using altered video or audio evidence that appears to contradict the claim."[8] Without more granular broadcast announcements about the use of AI-generated content in political ads, malicious political advertisers could exploit the Commission's proposed on-air announcement requirement to foster doubt about truthful statements (when paired with non-obvious AI-generated content) or engender trust in false or misleading AI-generated content (when paired with more obvious AI-generated content). In both scenarios, the public will be left unsure about what aspect(s) of a political ad are AI-generated—and what aspects to believe.

Second, the risks of the Liar's Dividend grow more likely as the public grows more aware of AI-generated content. As Chesney and Citron argue, a "skeptical public will be primed to doubt the authenticity of real audio and video evidence" as convincing AI-generated content becomes more common.[9] Without more granularity within its proposed broadcast announcement requirement, the Commission risks priming the American electorate to distrust wide swaths of truthful and politically salient content due to the specter of convincing AI deepfakes.

Under the Commission's current proposed rules, listeners and viewers do not have sufficient information from broadcasters to evaluate whether *politically salient* content within an ad is false, misleading, or otherwise fabricated. To overcome this information gap, EPIC urges the Commission to require broadcasters to inquire not only *whether* political ads contain AI-generated content, but also *how* those ads use AI-generated content. For example, a broadcaster could inquire whether a political ad includes AI-generated depictions of a candidate or AI-generated approximations of a public figure's voice. The Commission could then require broadcasters to incorporate this additional information into their required on-air announcements. Rather than require the statement, "the following message contains information generated in whole or in part by artificial intelligence," for example, the Commission could require broadcasters to include one of a set of more granular disclosure statements, such as: "The following message contains

[7] Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1785–86 (2019).
[8] *Id.* at 1785.
[9] *See id.*

audiovisual depictions of a political candidate generated in whole or in part by artificial intelligence."

III. The Commission Should Require Broadcasters to Inquire About the Presence of AI Watermarks in Political Ads and Retain that Information in Their Political Files

We appreciate the Commission's interest in requiring information concerning AI-generated content to be retained within broadcasters' political files required under 47 U.S.C. § 315(e). The Commission's political recordkeeping requirements are crucial avenues for increasing transparency and accountability over political advertising. To ensure the Commission's proposed rules are maximally effective, however, we urge the Commission to expand the information it requires broadcasters to inquire about and retain to include (1) the specific ways that political advertisers include AI-generated content outlined in Section II, *supra*, and (2) information concerning any AI watermarks or other content labels included within AI-generated content used for political ads.

AI watermarking or content labeling is the process of embedding information disclosures into AI-generated content. For example, an AI developer may require all images its AI models generate to include a visible label or watermark on top of the image. Similarly, watermarks or other means for authenticating content as AI-generated may be woven imperceptibly into AI-generated images, text, audio, or video such that content can be identified as AI-generated by technical systems even when they do not appear to have watermarks or labels. As described in NIST's Draft Document on Reducing Risks Posed by Synthetic Content,[10] currents methods for disclosing the existence and provenance of AI-generated content include:

1. content labels like visual tags or warning labels,
2. visible watermarks placed over AI-generated content,
3. disclosure fields such as acknowledgements provided alongside AI-generated content,
4. covert or imperceptible watermarks, which are hidden within AI-generated content but identifiable using technical processes,
5. digital fingerprints, and
6. embedded metadata.

These technical methods for disclosing AI-generated content, while nascent, have already garnered attention from lawmakers in the United States and abroad.[11] As AI watermarking

[10] NIST, Reducing Risks Posed by Synthetic Content, NIST AI 100-4, at 5 (2024), https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent.ipd.pdf (draft provided for public comment).

[11] *See, e.g.*, Ilana Beller, Public Citizen, *Tracker: State Legislation on Deepfakes in Elections* (Aug. 26, 2024), https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/; Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial

requirements grow more common, so too will the incidence of watermarks within AI-generated content used for political ads.

Requiring broadcasters to inquire about and retain information about AI watermarks or other content disclosure techniques is not only a natural extension of the Commissions' currently proposed requirements, but also an effective means for increasing public transparency around *how* AI-generated content is specifically used within political ads. Interested members of the American electorate—as well as civil society organizations and academic researchers—can do more to understand and evaluate political ads containing AI-generated content when they have direct access to AI watermarks and other disclosure documentation within broadcasters' political files. And while disclosures of AI watermarks can increase the risk that malicious actors will identify and remove or circumvent AI watermarks,[12] we believe the public benefits of disclosing the existence, type, or details of AI watermarks within broadcasters' political files outweighs the risks of further information manipulation or deception by malicious actors trying to identify, remove, or circumvent AI watermarks.

AI watermarking and similar methods of authenticating content as AI-generated are still imperfect means for mitigating the harms of false, misleading, or deceptive AI-generated content; researchers at the University of Maryland have already found several ways to break watermarking techniques and insert false watermarks onto AI images.[13] However, requiring broadcasters to inquire into and disclose the existence of AI watermarks remains an effective way to increase the granularity and transparency of the Commission's proposed disclosure rules surrounding AI-generated content in political ads. As discussed in Section II, *supra*, the value of public disclosures depends entirely on a listener or viewer's ability to effectively leverage that information to evaluate political messaging. Without ensuring that the public has access to specific information about what content is AI-generated and how that content is being used by political advertisers, the Commission cannot further the First Amendment's goal of an informed electorate.

IV. The Harms of AI-Generated Political Disinformation Warrant FCC Restrictions on Knowingly Broadcasting False, Misleading, or Deceptive AI-Generated Content

Beyond any proposed public disclosure rules, EPIC urges the Commission to reconsider its decision not to ban or restrict *any* use or broadcasting of AI-generated content in political ads. As FCC Commissioner Starks has already noted, generative AI technologies can supercharge political misinformation and disinformation in ways that produce real and significant harms to

Intelligence Act) and Amending Certain Union Legislative Acts, European Commission, COM(2021) 206 final, 2021/0106 at Art. 50, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (EU AI Act).

[12] *See* Generating Harms II Report at 20–21; Mehrdad Saberi et al., *Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks*, arXiv (Feb. 14, 2024), https://arxiv.org/pdf/2310.00076.

[13] *Id.*

consumers: scams, election threats, threats to public safety, and more.[14] For example, AI-generated audio, video, and images can warp public perceptions of candidates,[15] foment political unrest,[16] or mislead voters on where and when to vote.[17] When paired with microtargeted advertising campaigns, AI-facilitated political ads can surreptitiously distort what different voter demographics see and believe.[18] And at their worst, AI disinformation campaigns can fuel support for violent and unfounded conspiracy theories.[19]

Both the risks and features of AI disinformation resemble those of two separate practices that the Commission has already exercised its authority to restrain: hoaxes[20] and broadcast news distortion.[21] Under 47 C.F.R § 73.1217(a), for example, "no licensee or permittee of any broadcast station shall broadcast false information concerning a crime or catastrophe" if they knew the information was false, they could foresee that the broadcast would cause "substantial public harm," and the broadcast does, in fact, cause substantial public harm. Similarly, the FCC has stated that "rigging or slanting the news is a most heinous act against the public interest."[22]

When a broadcaster knowingly broadcasts false, misleading, or deceptive AI-generated content and the broadcast in turn causes substantial public harm or slants the news, the broadcaster squarely violates the Commission's restraints on hoaxes or news distortion, respectively. There is no meaningful distinction between restrained broadcast practices involving AI-generated content

[14] *See* Statement of Comm'r Geoffrey Starks, *In re* Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, CG Dkt. No. 23-362, Declaratory Ruling (Feb. 8, 2024), https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf/.

[15] *See* Morgan Meaker, *Slovakia's Election Deepfakes Show AI is a Danger to Democracy*, Wired (Oct. 3, 2023), https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/; Stuart A. Thompson, *Making Deepfakes Gets Cheaper and Easier Thanks to A.I.*, N.Y. Times (Mar. 12, 2023), https://www.nytimes.com/2023/03/12/technology/deepfakes-cheapfakes-videos-ai.html.

[16] *See Microsoft Finds Russian Influence Operations Targeting U.S. Election Have Begun*, Reuters (Apr. 17, 2024), https://www.reuters.com/world/us/microsoft-finds-russian-influence-operations-targeting-us-election-have-slowly-2024-04-17/; Dustin Volz, *China is Targeting U.S. Voters and Taiwan with AI-Powered Disinformation*, Wall St. J. (Apr. 5, 2024), https://www.wsj.com/politics/national-security/china-is-targeting-u-s-voters-and-taiwan-with-ai-powered-disinformation-34f59e21.

[17] *See* Maggie Astor, *Behind the A.I. Robocall that Impersonated Biden: A Democratic Consultant and a Magician*, N.Y. Times (Feb. 27, 2024), https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html; David Klepper & Ali Swenson, *AI Presents Political Peril for 2024 with Threat to Mislead Voters*, Associated Press (May 14, 2023), https://apnews.com/article/artificial-intelligence-misinformation-deepfakes-2024-election-trump-59fb51002661ac5290089060b3ae39a0.

[18] *See, e.g.*, Almog Simchon et al., *The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence*, 3(2) PNAS Nexus, Jan. 29, 2024, https://academic.oup.com/pnasnexus/article/3/2/pgae035/7591134.

[19] *See* Lorne Cook & Kelvin Chan, *AI Could Supercharge Disinformation and Disrupt EU Elections, Experts Warn*, Associated Press (June 5, 2024), https://apnews.com/article/eu-european-union-election-disinformation-43b7e4017825d9d382859894b7625e7a; Tiffany Hsu & Stuart A. Thompson, *Disinformation Researchers Raise Alarms About A.I. Chatbots*, N.Y. Times (June 20, 2023), https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html.

[20] 47 C.F.R. § 73.1217.

[21] The Media Bureau, FCC, The Public and Broadcasting: How to Get the Most Service from Your Local Stations, at 12 (2019) (presenting News Distortion Doctrine).

[22] *Id.*

and those involving other content—nor should there be. As the Commission considers methods to ensure that broadcasters and other regulated entities continue to serve the public interest when dealing with AI-generated content in political ads, we urge you not to turn a blind eye to the harms of AI-generated political disinformation or provide an AI carveout to regulated entities' statutory obligations.

V. Conclusion

We commend the Commission's efforts to safeguard the public from the harms of false, misleading, and deceptive AI-generated political content, and we urge the Commission to bolster its proposed disclosure requirements by increasing the clarity around what aspects of political messaging are AI-generated and by pairing on-air announcements with guidance around developing—and broadcasters inquiring about—audio and visual AI watermarks within political ads. The public needs effective means for identifying and evaluating AI-generated content, not just ads that contain AI-generated content. Without a more granular and durable method for identifying and evaluating AI-generated content, the Commission's proposed rule will be far less effective at deterring AI harms and fostering an informed electorate. EPIC believes not only that the Commission has the authority to make such an AI transparency and disclosure regime possible, but also that such a regime is the most effective way to promote the public interest and "preserv[e] the audience's right to know by whom it is being persuaded."[23] Additionally, we urge the Commission to reconsider its decision not to impose any restraints on the use of AI-generated content in political ads. Not only are the risks of AI political disinformation substantial, but AI political disinformation also resembles two forms of broadcast content—hoaxes and news distortion—that the FCC has already exercised its authority to restrain.

Respectfully submitted, September 4, 2024.

Grant Fergusson
Counsel
fergusson@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

[23] *Amendment of the Commission's Sponsorship Identification Rules*, Docket No. 19513, Report and Order, 52 FCC 2d 701, 711, para. 30 (1975).