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

***Filed online at fcc.gov/ecfs***

October 10, 2024

Marlene H. Dortch
Secretary
Federal Communications Commission
Office of the Secretary
45 L Street NE
Washington, DC 20554

**Re: Implications of Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls and Robotexts**

The Future of Privacy Forum ("FPF") encourages the Federal Communications Commission ("FCC" or "Commission") to continue investigating AI detection technologies, and in doing so, to consider technical and organizational safeguards to mitigate the privacy risks raised by tools intended to protect consumers from unwanted robocalls and robotexts. FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.[1]

On September 10, 2024, the FCC published a Notice of Inquiry ("NOI") on technologies that can alert consumers that they may be interacting with an AI-generated call.[2] Specifically, in the NOI, the FCC seeks comment on tools for detecting, alerting, and blocking AI-generated calls based on real-time phone call content analysis and the privacy implications of these technologies. AI detection technologies raise potential privacy risks. Additionally, as they are used today, these technologies have functional limitations. As such, we recommend that the Commission continue to evaluate their capabilities, potentials, and impacts, and consider what role privacy-enhancing technologies can play in mitigating risks.

## I. Regulators are developing various approaches to address the risks associated with "synthetic" or AI-generated content—such as AI-generated robocall and robotext

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board. *See* Future of Privacy Forum, *About FPF*, https://fpf.org/about.

[2] The NOI was published alongside a Notice of Proposed Rulemaking (NPRM) on the implications of AI in robocalls and robotexts. *See* Federal Communications Commission, *Implications of Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls and Robotexts* (CG Docket No. 23–362, FCC 24–84; FR ID 239002) (Sep. 10, 2024), https://www.federalregister.gov/documents/2024/09/10/2024-19028/implications-of-artificial-intelligence-technologies-on-protecting-consumers-from-unwanted-robocalls.

**material—and these responses should be cohesive and, when possible, complementary.**

The proliferation of large language models (LLMs) and other generative AI tools has facilitated an influx of synthetic content, also known as AI-generated content, referring to text, audio, video, or other media that is created or significantly altered by algorithms.[3] While synthetic content is not inherently harmful, and can contribute to improvements in a wide range of domains, it can also exacerbate a number of privacy and safety risks,[4] including those related to disinformation and misinformation, malicious impersonation, fraud, and synthetic non-consensual intimate imagery (NCII) and child sexual abuse material (CSAM).[5]

For example, a political consultant created AI-generated robocalls impersonating President Biden and discouraging people in New Hampshire from voting in the primary.[6] Separately, former President Trump reposted false AI-generated images of Taylor Swift endorsing him for president on his social media account.[7] Malicious actors also use AI to create deepfake NCII, particularly of women and girls and people from historically marginalized communities, which can be used to discourage their political and civic participation.[8]

Regulators are exploring ways to use their authority to address these emerging issues. The FCC, for example, fined the individual responsible for the AI-generated robocall impersonating President Biden $6 million, citing a violation of the Truth in Caller ID Act.[9] The FCC is also considering developing rules to require broadcasters, cable operators, satellite providers, and others to make on-air disclosures regarding any political ads containing AI-generated content on

---

[3] National Institute for Standards and Technology, *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency* (Apr. 2024), https://airc.nist.gov/docs/NIST.AI.100-4.SyntheticContent.ipd.pdf.

[4] Ramak Molavi Vasse'i and Gabriel Udoh, *In Transparency We Trust? Evaluating the Effectiveness of Watermarking and Labeling AI-Generated Content*, Mozilla Foundation (Feb. 26, 2024), https://foundation.mozilla.org/en/research/library/in-transparency-we-trust/research-report. *See also* Supra 1.

[5] *See* Supra 1. These risks are particularly salient for women, people of color, older adults, and other people from marginalized and vulnerable communities, who often face greater harm when targeted with abusive synthetic content. *See* Amber Ezzell, Comment to Federal Election Commission re: REG 2023-02 Artificial Intelligence in Campaign Ads, Future of Privacy Forum (Oct. 16, 2023), https://fpf.org/wp-content/uploads/2023/10/Future-of-Privacy-Forum-FEC-Comment-on-AI-in-Campaign-Ads-October-16-2023.pdf. *See also*: Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*, W.W. Norton (2022), pg. 39.

[6] Holly Ramer and Ali Swenson, *Political consultant behind fake Biden robocalls faces $6 million fine and criminal charges*, Associated Press (May 23, 2024), https://apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c.

[7] Elizabeth Wagmeister and Kate Sullivan, *Trump posts fake AI images of Taylor Swift and Swifties, falsely suggesting he has the singer's support*, CNN (Aug. 19, 2024), https://www.cnn.com/2024/08/19/politics/donald-trump-taylor-swift-ai/index.html.

[8] Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do.*, The New York Times (Jul. 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html.

[9] Federal Communications Commission, *FCC Fines Man Behind Election Interference Scheme $6 Million for Sending Illegal Robocalls that Used Deepfake Generative AI Technology* (Sep. 26, 2024), https://docs.fcc.gov/public/attachments/DOC-405811A1.pdf.

their platforms.[10] Separately but relatedly, the Federal Trade Commission (FTC) is currently considering rulemaking to prohibit the impersonation of individuals, including AI-driven impersonation, building on an existing rule banning impersonation of businesses and government officials.[11] In order to ensure that the regulatory response to this rapidly growing category of content is cohesive and complementary, the FCC should consider how any rulemaking regarding AI-driven robocalls and robotexts implicates or is implicated by other similar regulatory efforts.

## II. Techniques for authenticating content or detecting the presence of AI are largely new, and should be evaluated for efficacy, technical limitations, and privacy impacts.

Deploying AI detection and authentication techniques in phone calls—which would likely require recording and analyzing people's private phone conversations—inherently involves privacy risks, with or without consent.[12] One technical approach to addressing the aforementioned risks involves *authenticating* content, or verifying the source, history, and/or modifications to a piece of content.[13]

Real-time AI call detection, alerting, and blocking technologies, for example, are intended to distinguish between synthetic and non-synthetic voice content to help people determine if they're speaking with a live human, which may help ensure that they are best situated to protect themselves from any potential AI-assisted scams. However, these tools, which have been compared in principle to email spam filters,[14] are in a nascent stage of development, and there is little to no research regarding their effectiveness or impacts.[15] Additionally, the current technical limitations of authenticating content can also create other risks, such as inequitable outcomes or false promises of efficacy. These tools are largely still in the early stages of development and prone to accuracy errors, though we note that they are generally not widely used by consumers.

More investigation into these technologies is warranted to determine whether they are, in their current stage, "fit for purpose" in order to adequately address the challenges for which they're

---

[10] For FPF's comment in response, *see* Jameson Spivack, *Re: Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements*, https://fpf.org/wp-content/uploads/2024/09/867d56ae-cd8e-4713-98f9-b6556247409c.pdf.

[11] For FPF's comment in response, *see* Jameson Spivack, Beth Do, and Angela Guo, *Re: Proposed Amendments to Trade Regulation Rule on Impersonation of Government and Businesses ("Impersonation SNPRM")*, https://fpf.org/wp-content/uploads/2024/04/FPF_FTC_SNPRM_Impersonation_Comment.pdf.

[12] The NOI considers whether it would be appropriate to require AI detection and authentication tools disclose their presence to called parties. *Supra* 2.

[13] Information Technology Industry (ITI), *Authenticating AI-Generated Content: Exploring Risks, Techniques & Policy Recommendations* (January 2014), https://www.itic.org/policy/ITI_AIContentAuthorizationPolicy_122123.pdf.

[14] Paula Boyd and Jennifer L. Oberhausen, *Comment to Federal Communications Commission re: CG Docket No. 23-362*, Microsoft Corporation (Dec. 18, 2023), https://www.fcc.gov/ecfs/document/1219842001792/1.

[15] The record for this proceeding reflects existing examples of this technology. *See*, for example, Christopher L. Shipley, Comment to Federal Communications Commission re: CG Docket No. 23-362, INCOMPAS (Jan. 16, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10116138887190.

tasked, as well as any privacy and safety risks they might raise. While AI detection techniques can help protect consumers from fraud and deception, the FCC should consider potential adverse outcomes for consumers, particularly if there are explicit requirements to deploy these techniques prematurely. Low-accuracy tools have the potential to create results that are either over- and under-inclusive. An over-inclusive tool may inadvertently filter out real humans and prevent individuals from initiating or receiving calls. Over-inclusivity is likely to disproportionately impact specific groups, such as non-native English speakers.[16] An under-inclusive tool, on the other hand, may not accurately catch all the AI-generated content, which would undermine the goals of the FCC's efforts and could falsely reassure a consumer that a call is non-synthetic content.

At a minimum, FPF recommends that the Commission meet with a diversity of stakeholders, including relevant entities in industry, civil society, and academia, to discuss the current state of the technologies, their development trajectory, and potential risks and benefits of their use, including for historically marginalized communities. Considering these potential risks, it may be premature to establish specific requirements before the technology can be adequately evaluated. However, the FCC can still investigate the development of this technology, given its potential to alleviate complex issues regarding synthetic content. In continued investigations, the FCC should consider privacy mitigation strategies such as privacy-enhancing technologies, as discussed below.

## III. The FCC should investigate technical safeguards like confidential computing, as well as organizational practices like data minimization and purpose limitation, as possible means of mitigating some of the privacy risks raised by real-time call detecting, alerting, and blocking technologies

Certain privacy-enhancing technologies (PETs), while also relatively new, may prove capable of addressing some of the aforementioned privacy risks. For example, confidential computing, an emerging PET that isolates data processing within a computer's central processing unit (CPU) and prevents unauthorized access of data and processing activity, could allow detection, alerting, and blocking technologies to be implemented strictly for the purpose of determining the authenticity of the caller and without sharing any additional data.[17]

It bears repeating, however, that both content-based AI detecting, alerting, and blocking technologies, as well as PETs like confidential computing, are in their infancy. Should the

[16] Andrew Myers, *AI-Detectors Biased Against Non-Native English Writers*, Stanford University Human-Centered Artificial Intelligence (May 15, 2023), https://hai.stanford.edu/news/ai-detectors-biased-against-non-native-english-writers.
[17] Samuel Adams, Stacey Gray, Aaron Massey, and Rob van Eijk, *Confidential Computing and Privacy: Policy Implications of Trusted Execution Environments*, Future of Privacy Forum (July 2024), https://fpf.org/wp-content/uploads/2024/07/FPF-Confidential-Computing-Digital.pdf.

Commission decide to further explore AI detection, alerting, and blocking technologies in the context of private phone conversations, it should thoroughly investigate the current state of PETs and other tools being developed to allow secure data processing, and ensure that these tools adequately address the aforementioned privacy risks.

FPF appreciates the opportunity to comment on these issues, and the FCC's ongoing efforts to protect consumers from unwanted robocalls and fraudulent AI-driven activity. We welcome any further opportunity to provide resources or information to assist in this effort. If you have any questions regarding these comments, please contact Jameson Spivack at jspivack@fpf.org (cc: info@fpf.org).

Sincerely,

Jameson Spivack, Senior Policy Analyst
Bailey Sanchez, Senior Counsel

**Future of Privacy Forum**
https://fpf.org