Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts	)	CG Docket No. 23-362

COMMENTS OF CTIA

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Sarah Leggin
Assistant Vice President, Regulatory Affairs

Courtney Tolerico
Director, Regulatory Affairs

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, D.C. 20036

(202) 736-3200

October 10, 2024

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts	)	CG Docket No. 23-362

COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") Notice of Proposed Rulemaking and Notice of Inquiry[2] proposing to define "[Artificial Intelligence ("AI")]-generated calls" and subject those calls to specific pre- and on-call disclosure requirements and seeking additional information about developing technologies that can alert consumers to unwanted or illegal calls and texts.

I. INTRODUCTION AND SUMMARY.

The wireless industry is committed to leveraging innovative technologies like AI to facilitate legitimate communications and protect consumers from bad actors who would use AI for illegal robocalls and robotexts. CTIA commends the Commission for continuing a public dialogue regarding these important issues and seeking input on the appropriate framework for protecting consumers.

---

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless providers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 24-84 (rel. Aug. 8, 2024) ("*NPRM*" and "*NOI*").

The wireless industry is already responsibly leveraging AI in myriad applications throughout the wireless ecosystem for the benefit of consumers and other wireless users. CTIA and its member companies are mindful of both the benefits and risks of AI, and they are incentivized to strike the right balance in promoting innovative uses while protecting consumers. CTIA and its member companies also continue to work alongside other industry and government partners to develop practices and policies that will serve as the foundation of safe and responsible use of AI technologies.

CTIA supports the important steps the Commission has already taken to thwart the use of AI by bad actors. For instance, the February 2024 *Declaratory Ruling* in this proceeding clarified that AI technologies that resemble human voices and/or generate call content using prerecorded voice are already subject to the Telephone Consumer Protection Act ("TCPA") and the Commission's rules.[3] The *Declaratory Ruling* established clear guidance on the use of AI in illegal calls that has already helped the Commission and industry protect consumers from bad actors. Given these and other successful efforts by the Commission, industry, and other government partners to promote innovative technologies while effectively tackling evolving challenges, new regulations or legislation focused on addressing AI-enabled calls and text messages would be premature.[4]

Here, the *NPRM*'s proposals to define "AI-generated calls" and subject those calls to specific pre- and on-call disclosure requirements are not the most effective way to protect

[3] *See generally Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, Declaratory Ruling, FCC 24-17 (rel. Feb. 8, 2024) ("*Declaratory Ruling*").

[4] *See, e.g.*, Letter from Jordan Crenshaw, Senior Vice President, Chamber Tech. Engagement Ctr., Chamber of Com., to Marlene H. Dortch, Sec'y, FCC, CG Docket No. 23-362, at 1 (July 19, 2024), https://www.fcc.gov/ecfs/document/107192738018958/1 ("Chamber of Commerce Letter").

consumers from illegal AI-generated calls, particularly considering the Commission's existing efforts. At best, the *NPRM*'s proposals would unnecessarily duplicate the effects of the *Declaratory Ruling*. At worst, these proposals risk causing significant confusion for callers, providers, and consumers alike and ultimately chilling innovative uses of AI that would benefit callers and consumers.

Instead, the Commission should continue to collaborate with industry and other governmental entities as well as other stakeholders to promote innovative solutions and utilize its current enforcement tools to combat bad actors. For example, the Commission can enhance trust in voice calling, including calls made with AI technology, by supporting the development of tools like Rich Call Data ("RCD") and branded calling solutions. The Commission should also continue to align its efforts with other federal agencies, such as the National Institute of Standards and Technology ("NIST"), that are establishing the frameworks that will guide a risk-based approach to the use of AI. Further, the Commission should clarify the *Declaratory Ruling* to ensure that its interpretation of the TCPA does not hinder the use of AI technologies that enable people with disabilities to better access the telephone network.

Finally, with respect to the *NOI*, the Commission should proceed with care in exploring technologies that would detect illegal calls by, among other things, monitoring the content of calls. While these solutions could help identify illegal calls, they also raise significant questions about how to balance the need to protect consumer privacy with the Commission's consumer protection goals. CTIA encourages the Commission to continue evaluating the solutions described in the *NOI* collaboratively with industry before encouraging or directing their adoption.

II. THE WIRELESS INDUSTRY IS COMMITTED TO RESPONSIBLY LEVERAGING AI TO PROTECT AND BENEFIT CONSUMERS.

As CTIA has explained, the wireless industry is already leveraging AI to bring new use cases—and new protections—to consumers. CTIA and its member companies are cognizant of both the benefits and risks of AI. While AI technology can enable faster, smarter, and more effective communication, it may also enhance or facilitate scams by bad actors. To that end, the wireless industry has engaged with industry and government partners to promote thoughtful, risk-based approaches that maximize the benefits and minimize the risks of AI for consumers.

A. The Wireless Industry Continues to Develop and Use AI Technologies to Enhance Wireless Services and Protect Consumers from Illegal Calls.

In fewer than ten months since CTIA last outlined the wireless industry's efforts to leverage AI capabilities to promote network and service enhancements and efficiencies to the benefit of consumers, CTIA and its member companies have contributed to new developments in the field that have accelerated leveraging the benefits of AI for networks and consumers across the country.

Last December, CTIA highlighted that wireless providers were already using AI to "(i) analyze vast quantities of network data, identify patterns, and predict outcomes to avoid network outages; (ii) prevent fraud; (iii) provide virtual assistance with AI-based natural language processing, customer engagement tools, intelligent routing, interactive voice response, webforms, and bots; (iv) optimize product delivery; (v) enable climate risk planning; and more."[5] In less than a year since those comments, CTIA's member companies have continued to expand these capabilities and add new ones. For example, AT&T's AI-enabled "autonomous

[5] Comments of CTIA, CG Docket No. 23-362, at 4–5 & nn.9–18 (Dec. 18, 2023) ("CTIA NOI Comments").

assistants" can take "fraud alerts . . . and stop a fraudulent transaction before it happens" and can support an employee on a customer call by "work[ing] behind the scenes to almost instantly analyze that customer's account and provide a menu of options that [the] employee can present to that customer."[6] T-Mobile recently announced a collaboration with NVIDIA, Ericsson, and Nokia to invest in AI-radio access networks, or "AI-RAN," which "will dramatically improve customers' real-world network experiences and ever-growing demand for increased speeds, reduced latency, and increased reliability."[7] And Verizon also uses AI technologies to help customer service representatives more quickly troubleshoot and identify solutions for customers, as well as protect and prevent damage to its fiber infrastructure.[8]

At the same time, CTIA's member companies have remained at the forefront of protecting consumers from risks associated with AI technology used by bad actors. Among other things, the wireless industry has continued to implement and enhance processes, tools, and best practices to help protect consumers from spam and scam calls and text messages, regardless of the technology used by bad actors. Many of these processes and tools leverage AI to protect consumers.[9]

---

[6] Andy Markus, *Autonomous Assistants: The Next Step of the GenAI Revolution to Empower Employees and Serve Customers*, AT&T BLOG (July 17, 2024), https://about.att.com/blogs/2024/autonomous-assistants.html.

[7] Press Release, T-Mobile, T-Mobile Announces Technology Partnership with NVIDIA, Ericsson and Nokia to Advance the Future of Mobile Networking with AI at the Center (Sept. 18, 2024), https://www.t-mobile.com/news/business/t-mobile-launches-ai-ran-innovation-center-with-nvidia.

[8] Verizon, Verizon Uses AI & Machine Learning to Prevent Fiber Cuts (Aug. 7, 2024), https://www.verizon.com/about/news/verizon-uses-ai-machine-learning-prevent-fiber-cuts.

[9] *Id.* at 5–7; Reply Comments of CTIA, CG Docket Nos. 21-402, 02-278, & 17-59, at 5–10 (Mar. 11, 2024).

B. The Wireless Industry Is Working Alongside Government and Industry Partners to Promote Safe and Responsible AI Deployment.

The wireless industry is an active participant in government and cross-industry efforts to promote safe and responsible development and deployment of AI technologies. For example, CTIA's member companies are active participants in the Biden Administration's effort to "counter fraudsters who are using AI-generated voice models to target and steal from the most vulnerable in our communities."[10] This year, representatives from CTIA, AT&T, T-Mobile, and Verizon attended a roundtable discussion hosted by officials from the Administration that featured Chairwoman Rosenworcel, Federal Trade Commission ("FTC") Chairwoman Lina Khan, and representatives of AI technology companies, consumer advocates, academia, and others to "discuss the state of AI-generated voice cloning technology and how we can work together to develop viable solutions to combat AI-generated robocalls."[11] CTIA has continued to participate in these Administration-led, cross-sector sessions that are exploring ways to collaborate and promote innovative uses of AI while continuing to protect consumers.

CTIA has engaged with other agencies on this issue, too. CTIA participated in NIST's development of the AI Risk Management Framework ("AI RMF")[12] and contributed to the White House Office of Science and Technology Policy's ("OSTP") National Priorities for AI.[13] CTIA and its member companies contributed to NTIA's efforts to implement the measures

---

[10] Press Release, White House, FACT SHEET: Vice President Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence (Nov. 1, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/fact-sheet-vice-president-harris-announces-new-u-s-initiatives-to-advance-the-safe-and-responsible-use-of-artificial-intelligence/.

[11] Maggie Miller, *White House Convenes Meeting on AI Voice Cloning*, POLITICO PRO (Feb. 6, 2024), https://subscriber.politicopro.com/article/2024/02/white-house-convenes-meeting-on-ai-voice-cloning-00139947.

[12] CTIA NOI Comments at 8; *See* Comments of CTIA, NIST Docket No. 210726-0151 (Sept. 15, 2021); Comments of CTIA, NIST AI Risk Management Framework (Sept. 29, 2022).

[13] *See generally* Comments of CTIA, Docket ID: OSTP-TECH-2023-0007 (July 7, 2023).

required by the AI Executive Order.[14] And, CTIA and its member companies also support other whole-of-government efforts to tackle the problem of spam and scam calls and texts that may use AI, including the FTC's voice cloning challenge and its work to adopt rules to enhance enforcement against impersonation fraud.[15]

Additionally, the wireless industry contributed to the Commission's Consumer Advisory Committee's ("CAC") recent report and recommendations examining the uses of AI to protect consumers from unwanted robocalls, robotexts, and other harms, and to enable people with disabilities to better utilize the telephone network.[16] CTIA and several of its' member companies will also participate in the Commission's recently-reconvened Communications Security, Reliability, and Interoperability Council ("CSRIC"), which is tasked with developing recommendations on "the reliability of communications systems and infrastructure," including discussions of means to safeguard the public from malicious uses of AI.[17]

CTIA and its member companies look forward to further working with the Commission and other government partners on these foundational workstreams to embrace opportunities and tackle challenges presented by AI.[18]

---

[14] *See generally* Comments of CTIA, Docket No. 230407-0093, NTIA-2023-07776 (June 12, 2023).

[15] Press Release, FTC, FTC Announces Winners of Voice Cloning Challenge (Apr. 8, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge ("FTC Voice Cloning Winners Press Release"); Trade Regulation Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15017 (Mar. 1, 2024) (to be codified at 16 C.F.R. pt. 461); Trade Regulation Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15072 (Mar. 1, 2024).

[16] *See generally Consumer Advisory Committee Meeting, September 24*, FCC, https://www.fcc.gov/news-events/events/2024/09/consumer-advisory-committee-meeting-september-24 (last visited Oct. 8, 2024) ("CAC Meeting Recording"). The report containing these recommendations was approved and adopted by the CAC at its September 24 meeting. *Id.* at 1:29:48-1:29:50.

[17] *See Communications Security, Reliability, and Interoperability Council*, FCC, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Oct. 8, 2024).

[18] CTIA NOI Comments at 10.

III. COORDINATION AMONG GOVERNMENT AND INDUSTRY WILL MORE EFFECTIVELY ENHANCE TRUST AND MITIGATE AI RISK THAN IMPOSING TECHNOLOGY-SPECIFIC OBLIGATIONS.

It is unnecessary and, at best, premature for the Commission to adopt the proposals in the *NPRM*. The Commission has already taken significant and effective steps—most notably, the *Declaratory Ruling*—to combat illegal robocalls and robotexts made using AI technologies that present "an enhanced risk of fraud and other scams."[19] Caution is especially warranted here, where the Commission's proposals risk causing significant confusion for consumers, callers, and providers and chilling innovation that would otherwise drive beneficial developments and use cases for AI. CTIA urges the Commission to defer the technology-specific regulations proposed in the *NPRM* and focus its efforts on coordinating with industry and government partners to promote solutions that will enhance trust in calling and maintain consumer trust in text messaging.

A. The *NPRM*'s Proposals to Define "AI-Generated Calls" and to Impose Additional Consent and Disclosure Requirements on Those Calls Are Unnecessary and Risk Generating Confusion and Chilling Innovation.

Just eight months ago, the Commission made clear that "the TCPA's restrictions on the use of 'artificial or prerecorded voice' encompass current AI technologies that generate human voices."[20] Based on the Commission's decision, consumers already have the same protection from calls made using "voice cloning" technology, deepfakes, or other similar AI-generated technologies that fall within the scope of the TCPA.[21] No additional Commission action is necessary.

---

[19] *NPRM* ¶ 2.

[20] *Declaratory Ruling* ¶ 2.

[21] Chamber of Commerce Letter at 3. Public perception of the *Declaratory Ruling* confirms its effect. *See, e.g.*, Kate Gibson, *FCC Declares AI-Generated Voices in Robocalls Are Illegal*, CBS NEWS (Feb. 8, 2024), https://www.cbsnews.com/news/fcc-declares-robocalls-illegal/.

The Commission has also already proven that it can leverage the *Declaratory Ruling* for consumer protection, as evidenced by its recent enforcement action against the bad actor behind the deepfake political robocalls made during the 2024 New Hampshire primary election.[22] This action against a bad actor using AI to enhance the potency of robocall fraud proves that the Commission's existing enforcement tools and existing industry frameworks—like the Industry Traceback Group,[23] in which CTIA's member companies participate—can be used to protect consumers from AI-enhanced threats.

Despite these effective steps, the *NPRM* proposes to create a new definition of "AI-generated" calls and impose specific pre- and on-call disclosure requirements on these "AI-generated calls."[24] These proposals suffer from two key flaws.

First, proceeding with this approach will only create uncertainty for lawful callers, lawful texters, and consumers alike. Lawful callers and texters will be unsure of the extent to which their "artificial" calls and texts are covered by the Commission's proposed definition and may make different choices about which calls require the unique disclosures that would be required under the *NPRM*. This may leave consumers unable to accurately discern which calls and texts they are consenting to and which calls they receive are "AI-generated" (and disclosed) or are potentially otherwise "artificial" (and are undisclosed). The lack of clarity will further encourage parties to seek judicial interpretations of the Commission's rules under the TCPA. If, as appears

---

[22] *See* Press Release, FCC, FCC Fines Man Behind Election Interference Scheme $6 Million for Sending Illegal Robocalls that Used Deepfake Generative AI Technology (Sept. 26, 2024), https://docs.fcc.gov/public/attachments/DOC-405811A1.pdf (noting that the FCC recently confirmed that the TCPA's restrictions on calls using an "artificial or prerecorded voice" apply to calls using AI-generated voices).

[23] *See About: What is the Industry Traceback Group?*, Industry Traceback Group, https://tracebacks.org/about/ (last visited Oct. 8, 2024).

[24] *NPRM* ¶¶ 10, 14. CTIA supports the *NPRM*'s clarification that texting is exempt from the on-call disclosure requirement. *Id.* ¶ 11 n.36.

to be the case, the Commission does not intend to capture all "artificial" or prerecorded calls,[25] this uncertainty risks leading to conflicting judicial interpretations of the Commission's rules that will negatively impact lawful callers and texters.[26]

Second, this uncertainty risks stifling innovative uses of AI in ways that may harm callers and consumers. As discussed above, AI has enormous potential to beneficially impact callers, senders, and consumers. Adding new hurdles and potential liability risk for lawful callers will only make them less likely to experiment with new ways to reach and connect with consumers. In turn, consumers may miss out on numerous improvements to their experiences.

Ultimately, as many commenters have already pointed out in the Commission's related proceeding that proposes to impose disclosure obligations on the use of AI in political advertisements,[27] premature regulatory action may lead to unintended consequences, particularly when it comes to nascent technologies like AI.[28] Instead, the Commission should promote and

---

[25] *See NPRM* ¶ 13 (asking, "[i]f we do not define an AI-generated call in this context, how would callers determine whether the disclosure obligations proposed below apply to the calls and texts messages that they are sending?"). This implies that the Commission intends the definition to capture a subset of calls already within the scope of the *Declaratory Ruling*.

[26] *See* Shay Dvoretzky et al., *The Evolving Telephone Consumer Protection Act Landscape Post*-Duguid, SKADDEN: SKADDEN INSIGHTS – APRIL 2022 (Apr. 2022), https://www.skadden.com/insights/publications/2022/04/quarterly-insights/the-evolving-telephone-consumer-protection-act (explaining that recent judicial and FCC decisions, "combined with a prolific plaintiffs' TCPA bar, have resulted in an onslaught of class actions").

[27] *See generally Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements*, Notice of Proposed Rulemaking, FCC 24-74 (rel. July 25, 2024).

[28] *See, e.g.*, Comments of Taxpayers Protection Alliance, MB Docket No. 24-211, at 4 (Sept. 19, 2024) ("the FCC's proposal [to require disclosures on 'AI-generated' content in political ads] would, if finalized, drive technologists and users away from AI products — for no good reason. The problem the FCC seeks to address is the potential that nefarious actors will use technology to . . . mislead Americans. This concern is not specific to AI-based tools. Nor will it be solved by the proposed disclosures."); Comments of Jennifer Huddleston et al., MB Docket No. 24-211, at 2 (Sept. 6, 2024) (explaining that disclosures may increase consumer confusion and mistrust and risk driving providers away from beneficial and efficient AI tools); Comments of the Center for Data Innovation, MB Docket No. 24-211, at 5 (Aug. 23, 2024) (explaining that "AI-generated content is not necessarily deceptive so these disclosures may confuse voters").

monitor the ways AI may enhance and improve consumer experiences with voice calls and text messages.[29] To the extent that the Commission sees potential risks, it can leverage existing authority, such as the *Declaratory Ruling*, which is sufficiently flexible to combat misleading and fraudulent AI-generated calls that are the true target of this proceeding.[30]

B. The Commission Should Coordinate with Government and Industry Efforts to Enhance Trust in Calling That Will Help to Mitigate AI Risk.

In lieu of the *NPRM's* proposals, CTIA encourages the Commission to focus on building trust in voice calls and maintaining trust in text messaging by supporting the development of new technologies and solutions and furthering its coordination and partnership with industry and other government stakeholders. This approach would be consistent with the recent recommendations of the Commission's CAC.[31]

For example, the Commission should encourage the development of industry solutions, such as branded calling and RCD. CTIA has previously explained that branded calling "includes a wide range of call authentication tools that leverage STIR/SHAKEN—along with a variety of

---

[29] *See* CAC Meeting Recording at 36:42-38:00 (recommending that the Commission "continue to support voice service providers' deployment of current and additional tools and processes to identify, block, label (as appropriate), and otherwise mitigate illegal and unwanted calls and texts, including any such calls and texts that are AI-generated").

[30] As CTIA has previously highlighted, several other federal agencies have concluded that they may already be able to apply existing legal frameworks to certain AI-related activities. *See* CTIA NOI Comments at 11 (discussing such conclusions made by the Consumer Financial Protection Bureau, Department of Justice, Equal Employment Opportunity Commission, and the FTC); *see also* Press Release, Fed. Election Comm'n, FEC Approves Two Advisory Opinions, Final Rule on Candidate Security, Notice of Disposition of Rulemaking, and Interpretive Rule (Sept. 20, 2024), https://www.fec.gov/updates/fec-approves-two-advisory-opinions-final-rule-on-candidate-security-notice-of-disposition-of-rulemaking-and-interpretive-rule/.

[31] *See* CAC Meeting Recording at 32:09-33:36, 36:42-38:00 (recommending, among other steps, that the Commission a) "partner with other federal agencies and the White House to ensure that there is a comprehensive solution across all agencies that helps prevent AI from being used for malicious calling purposes" and b) "continue to support voice service providers' deployment of current and additional tools and processes to identify, block, label (as appropriate), and otherwise mitigate illegal and unwanted calls and texts, including any such calls and texts that are AI-generated").

other data sources—to enhance the information that is displayed to a consumer when they receive a call."[32] CTIA is currently developing an RCD-based service called Branded Calling ID ("BCID") and looks forward to an opportunity to update the Commission on the myriad benefits of this solution.[33] By supporting a secure, ecosystem-based approach to verifying legitimate callers, CTIA's BCID can display caller, logo, and call reason information to consumers to help empower them to make more informed decisions about which calls to answer, which in turn can help consumers detect and avoid illegal AI-generated robocalls. These solutions show promise in enhancing the calling experience for consumers by building trust in voice calls, and the Commission can continue to encourage their development.

The Commission can also continue to leverage public-private partnerships to share information about and track down the bad actors behind robocalls and robotexts, including scams that are enhanced by AI technologies. For example, CTIA has been hard at work through the Secure Messaging Initiative ("SMI") to protect consumers by sharing information and enhancing partnerships with law enforcement – including the Commission, FTC, and the states – to crack down on bad actors, including those that appear to be leveraging AI to enhance their scams. CTIA's SMI has already made eleven referrals to the FCC, FTC, and the state Attorney Generals' enforcement task force, which included two referrals of scammers that appear to have used generative AI in their text message scam campaigns. CTIA encourages the Commission and its enforcement partners to leverage their existing tools to pursue these referrals and take action against these suspected bad actors.

[32] Comments of CTIA, CG Docket No. 17-59 & WC Docket No. 17-97, at 4 (Aug. 9, 2023) (internal citation omitted) ("CTIA Call Blocking *FNPRM* and *NOI* Comments").

[33] *Id.* at 5–6.

Additionally, the Commission should coordinate with other expert agencies, such as NIST, which has "significant and historical expertise in AI governance that can assist in the Commission's understanding of AI risks."[34] The guardrails that NIST is establishing for the use of AI overall will help to mitigate the harms posed by AI-generated robocalls. As CTIA has previously explained, the NIST AI RMF addresses definitions, metrics, and characterizations for AI risk in common language to facilitate adoption across diverse stakeholders.[35] The AI RMF forms the basis for the federal government's approach to AI risk management. It provides a framework for the "responsible design, development, deployment, and use of AI systems over time," and should serve as a guide for the Commission in its approach to AI issues writ large, which can then inform the Commission's approach in specific topic areas like this one.[36]

NIST also recently released its "Generative Artificial Intelligence Profile" ("NIST Generative AI Profile" or "Profile"), a companion document to the AI RMF that "defines risks that are novel to or exacerbated by the use of" generative AI and "provides a set of suggested actions to help organizations govern, map, measure, and manage these risks."[37] The Profile represents NIST's careful consideration of specific risks posed by generative AI and was informed by input from numerous stakeholders, including CTIA.[38] It appropriately focuses on enhancing government understanding of the responsible development and deployment of AI

[34] *See* Chamber of Commerce Letter at 3.

[35] CTIA NOI Comments at 10; *see NPRM* ¶ 46 (asking about the applicability of the NIST RMF and how it can be used to further the Commission's understanding of the risks posed by AI).

[36] NIST, NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), at 2 (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[37] NIST, NIST.AI.600-1: Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, at 1 (July 2024), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf ("NIST Generative AI Profile").

[38] Comments of CTIA, NIST Docket No. NIST-2024-0001 (dated June 1, 2024).

systems, the necessary precursor to any regulatory action.[39] As such, like the overall AI RMF, the NIST Generative AI Profile can further guide the Commission on how best to consider and approach the specific risks posed by generative AI in a holistic manner.

These efforts to better identify callers and set guardrails around the use of AI can together support the Commission's goal of enhancing consumer trust in calling and maintaining trust in text messaging. CTIA welcomes the opportunity to continue engaging with the Commission in developing thoughtful means to promote consumer trust in the calling and texting ecosystems.

C. The Commission Should Encourage the Use of AI Technologies to Facilitate Communications by People with Disabilities.

CTIA and its member companies have long supported Commission policies that help to facilitate access to communications services by people with disabilities. Given the revolutionary benefits of AI technologies for people with disabilities, CTIA agrees with the Commission and advocates for people with disabilities that the TCPA and the Commission's rules should not be an impediment to the legitimate use of AI technologies by people with disabilities.[40]

As the Commission acknowledges in the *NPRM*, some parties have expressed concern that the broad interpretation adopted in the *Declaratory Ruling* may unintentionally capture within the TCPA's prohibitions certain AI technologies that are beneficial to people with disabilities.[41] CTIA encourages the Commission to clarify the *Declaratory Ruling* to ensure that

[39] *See* NIST Generative AI Profile at 47–53.

[40] *See NPRM* ¶ 19.

[41] *See id.*; Letter from Karen Peltz Strauss, Legal Consultant, Voiceitt, to Marlene H. Dortch, Sec'y, FCC, CG Docket No. 23-362, at 2 (filed Mar. 1, 2024) (asking the "the Commission to exempt people using . . . computer-generated assistive speech technologies from TCPA mandates"); *see also* Letter from Margot Saunders, National Consumer Law Center, to Marlene Dortch, Sec'y, FCC, CG Docket No. 23-362, at 1 (filed Sept. 24, 2024) ("NCLC Letter").

it does not hinder the beneficial use of AI technologies "designed to assist individuals with disabilities to communicate by voice over the telephone network."[42]

The alternative approach outlined in the *NPRM* to clarify the definition of "artificial or pre-recorded voice" shows promise to accomplish this goal while ensuring that the TCPA can still be applied consistently.[43] At the same time, any definitions or exceptions to the TCPA and the Commission's rules should be considered carefully in order to avoid opening significant loopholes and risking practical issues in implementation.[44] CTIA encourages the Commission to strike the right balance between facilitating the use of AI to enhance access to communications for people with disabilities and protecting consumers from illegal calls that use AI voices.

IV. PRIVACY CONSIDERATIONS MUST BE PARAMOUNT WHEN EXPLORING TECHNOLOGIES THAT WOULD DETECT THE USE OF AI IN REAL TIME.

The Commission should remain cautious about whether to take steps that would encourage the development and deployment of network- or device-level technologies that can: "1) detect incoming calls that are potentially fraudulent and/or AI-generated based on *real time analysis of voice call content*; 2) alert consumers to the potential that such voice calls are fraudulent and/or AI-generated; and 3) potentially block future voice calls that can be identified as similar AI-generated or otherwise fraudulent voice calls based on analytics."[45]

---

[42] *NPRM* ¶ 29. *See* CAC Meeting Recording at 42:15-43:09 (recommending that the Commission "take all steps within its authority to ensure that its robocall regulations do not deter development and use of AI-powered tools that enable people with disabilities to better use the telephone network").

[43] *See NPRM* ¶¶ 29–30 (seeking comment on "whether we can define 'artificial or prerecorded voice' in a way that excludes from the requirements of the TCPA the use of technologies that are designed to assist individuals with disabilities to communicate by voice over the telephone network.").

[44] *See id.* ¶ 30 (inquiring how the Commission can ensure that it does not inadvertently "create a loophole that could be used by telemarketers or bad actors to circumvent the TCPA's protections"); *see also* CAC Meeting Recording at 42:15-43:09 ("[W]e recommend that the Commission ensure that these exemptions cannot be exploited by bad actors.").

[45] *NOI* ¶ 35 (emphasis added).

Today, wireless providers use reasonable analytics-based tools to identify and block illegal robocalls and advanced filtering tools to identify and block spam and scam messages before they reach consumers.[46] Wireless providers take seriously their obligations to protect consumer privacy and balance that goal with protecting consumers from unwanted and illegal calls and text messages. To do so, in the robocall space, call volume analytics and filtering tools are applied to identify and block illegal robocalls based on a variety of indicators.[47]

The wireless industry is constantly developing new technologies and solutions that will help further protect consumers from illegal robocalls and robotexts, particularly as bad actors seek to leverage AI to harm consumers. For example, the FTC's recent "voice cloning" challenge has identified a few solutions that may be able to detect and help providers block AI-generated calls from bad actors.[48] However, as the *NOI* notes, some of these solutions may require the real-time analysis of call content.[49] As the Commission recognizes, these technologies "pose *significant* privacy risks" and require careful development and analysis before they can be considered for use in networks.[50] CTIA and its member companies believe it would be premature to adopt such a requirement without further analysis of the privacy implications of such solutions.

---

[46] *See, e.g.*, CTIA NOI Comments at 2; Comments of CTIA, CG Docket Nos. 21-402 & 02-278, at 4–7 (May 8, 2023); Comments of CTIA, CG Docket Nos. 21-402, 02-278 & 17-59, at 6–7 (Feb. 26, 2024); CTIA Call Blocking *FNPRM* and *NOI* Comments at 11–18; Comments of CTIA, WC Docket No. 17-59, at 10 (Aug. 31, 2020).

[47] *See* Comments of CTIA, GN Docket No. 24-119, at 63–65 (June 6, 2024); CTIA NOI Comments at 5–6.

[48] FTC Voice Cloning Winners Press Release; *see* Comments of FTC, CG Docket No. 23-362, at 10–12 (July 29, 2024).

[49] *NOI* ¶¶ 38–39.

[50] *Id.* ¶ 38; *see also* CAC Meeting Recording at 38:01-39:19 ("The CAC recommends that the Commission consider how risks to privacy and compliance with privacy laws may be impacted by the use of call detection and alerting technologies that monitor the content of calls made to consumers.").

Other practical concerns about the Commission's *NOI* also require further consideration. It is unclear whether Commission guidance or direction is necessary or helpful to determine what providers are meant to do once these real-time identification technologies detect a voice clone call. For example, a broad Commission directive to use these technologies to block illegal calls could create confusion about whether such blocking should occur at the network or device level. And it is not clear from the *NOI* whether the Commission would require that detection of AI-generated call content trigger a special alert for the called party, and how such an alert would be implemented. The Commission's proposed approach to this issue must be more clearly articulated before affected parties can provide meaningful comment.

The Commission's call blocking rules alongside industry best practices and voluntary blocking efforts represent the outcome of long, careful consideration to facilitate trusted voice calling and text messaging ecosystems. While solutions presented in the *NOI* may similarly add new and possibly effective tools to providers' arsenals to thwart illegal robocalls and robotexts, premature and prescriptive steps by the Commission may hamper or warp the development process and cause these solutions to be less helpful—and possibly even harmful to legitimate callers and message senders. At this time, the Commission should monitor the development of these solutions before considering further action.

V. CONCLUSION.

The Commission has already taken significant strides toward protecting consumers from AI-enhanced illegal robocalls and robotexts, and it can leverage its *Declaratory Ruling* and other tools to further those goals. As discussed above, it is unnecessary and premature for the Commission to take further steps here, particularly when they risk creating uncertainty and chilling innovation that would otherwise benefit callers and consumers. CTIA looks forward to continuing to work with the Commission and other government and industry partners to monitor

developments in the use of AI in calling and text messaging and take steps that promote beneficial use cases while protecting consumers from bad actors.

Respectfully Submitted,

/s/ *Sarah Leggin*

Sarah Leggin
Assistant Vice President, Regulatory Affairs

Umair Javed
Senior Vice President and General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

Courtney Tolerico
Director, Regulatory Affairs

Mike Beirne
Director, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, D.C. 20036

(202) 736-3200

October 10, 2024