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
	)	
	)	

NOTICE OF INQUIRY

Adopted: November 15, 2023 **Released: November 16, 2023**

Comment Date: December 18, 2023
Reply Comment Date: January 16, 2024

By the Commission: Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

I. INTRODUCTION

1. In this *Notice of Inquiry* (*NOI*), we seek to better understand the implications of emerging artificial intelligence (AI) technologies as part of our ongoing efforts to protect consumers from unwanted and illegal telephone calls and text messages under the Telephone Consumer Protection Act (TCPA).[1] Complaints regarding unwanted and illegal robocalls and robotexts are consistently the top category of consumer complaints that we receive.[2] As a result, it is critical that the Commission stay abreast of new technologies that may impact the privacy protections afforded to consumers under the TCPA.

2. In the spirit of our longstanding efforts to protect consumers from unwanted robocalls, this *NOI* represents an opportunity to gather information and prepare for changes in calling and texting practices that may result from new AI-influenced technologies.[3] Specifically, we seek to understand how these technologies might affect the existing regulatory landscape that protects consumers from unwanted and illegal robocalls and robotexts. In this context, we seek information that could inform policies that anticipate how AI could help protect consumers against unwanted communications and how it could do the opposite. Our inquiry includes defining AI in this context, the current state of AI use in calling and texting, the impact of emerging AI technologies on consumer privacy rights under the TCPA, and, if appropriate, the Commission's next steps to address these issues.

II. BACKGROUND

3. The TCPA protects consumers from unwanted calls made using an artificial or prerecorded voice.[4] The legislative history of the TCPA suggests that Congress considered calls

[1] *See* Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394 (1991), *codified at* 47 U.S.C. § 227.

[2] The Commission received approximately 157,000 TCPA-related complaints in 2020, 164,000 in 2021, 119,000 in 2022, and 77,420 in 2023 as of Oct. 23, 2023. FCC, *Consumer Complaint Data Center*, www.fcc.gov/consumer-help-center-data (last visited Oct. 23, 2023).

[3] As discussed in more detail below, the TCPA regulates any call made using an "automatic telephone dialing system" or containing an artificial or prerecorded voice. Any such call is considered a "robocall" or "robotext" for purposes of this proceeding. *See* 47 U.S.C. § 227(b)(1).

[4] *See* 47 U.S.C. § 227(b)(1).

containing artificial and prerecorded voices to be a greater nuisance and invasion of privacy than calls using "live" persons.[5] As a result, the TCPA prohibits initiating "any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party" unless a statutory exception applies or the call is "exempted by rule or order by the Commission under [section 227(b)(2)(B)]."[6] The TCPA also prohibits, without the prior express consent of the called party, any non-emergency call made using an automatic telephone dialing system or an artificial or prerecorded voice to certain specified categories of telephone numbers including emergency lines and wireless numbers.[7] The Commission has confirmed that a text message is a "call" subject to the TCPA.[8]

4. The TCPA also authorizes the Commission to "prescribe technical and procedural standards for systems that are used to transmit any artificial or prerecorded voice message via telephone."[9] In addition, the legislative history of the TCPA supports the understanding that Congress anticipated that the Commission would have the flexibility to apply the TCPA's privacy protections from unwanted robocalls to future technologies as well as existing technologies.[10] In recent years, the federal government has begun to address emerging AI technologies, including a recent Executive Order.[11] These initiatives are designed to prepare for and manage the risks to society associated with these evolving technologies.[12]

---

[5] *See, e.g. Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, CC Docket No. 92-90, Notice of Proposed Rulemaking and Memorandum Opinion and Order, 17 FCC Rcd 17459 at 17473-74, para. 24 (citing S. REP. No. 102-178, at 2 (1991)) (2002).

[6] 47 U.S.C. § 227(b)(1)(B). The TCPA does not define the terms "artificial" or "prerecorded voice."

[7] *See* 47 U.S.C. § 227(b)(1)(A).

[8] *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14115, para. 165 (2003) (*2003 TCPA Order*); *see also Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946 (9th Cir. 2009) (noting that text messaging is a form of communication used primarily between telephones and is therefore consistent with the definition of a "call").

[9] 47 U.S.C. § 227(d)(3).

[10] *See* 137 Cong. Rec. S18784 (1991) (statement of Sen. Hollings) ("The FCC is given the flexibility to consider what rules should apply to future technologies as well as existing technologies"). The Commission's interpretation of the TCPA has accounted for new technologies that fell within its scope. *See, e.g.*, *Rules and Regulations Implementing the Telephone Consumer Protection Act*, *Westfax Inc. Petition for Consideration and Clarification*, CG Docket Nos. 02-278, 05-338, Declaratory Ruling, 30 FCC Rcd 8620 (2015) (confirming that an "efax," a document sent as a conventional fax but then converted and delivered as an electronic email attachment was covered by the TCPA's consumer protections from unwanted junk faxes).

[11] *See, e.g.,* The White House, U.S. Office of Science and Technology, Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People, https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (discussing "five principles that should guide the design, use, and deployment of automated systems to protect the American public" and citing "From Principles to Practice—a handbook . . .[that includes] detailed steps toward actualizing these principles in the technological design process") https://www.whitehouse.gov/ostp/ai-bill-of-rights/#applying ("This framework describes protections that should be applied with respect to all automated systems that have the potential to meaningfully impact individuals' or communities' exercise of: Rights, Opportunities, or Access."); U.S. Department of Commerce, National Institute of Standards and Technology, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework ("In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with artificial intelligence (AI). The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems"); Executive Order No. 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 88 Fed. Reg. 75191 (Oct. 30, 2023).

[12] *See, e.g.*, AI RMF.

III. DISCUSSION

5. As AI technologies that can generate content become increasingly prevalent, they have the potential to perform tasks that would ordinarily require human participation. These include interactive communications by voice calls and texts with consumers that can be beneficial. These technologies, however, can also pose new privacy and safety challenges. In this *NOI*, we explore the potential implications of emerging AI technologies on the privacy rights afforded to consumers under the TCPA.

6. Specifically, we seek comment on how AI technologies can be defined in the context of robocalls and robotexts, request information on how AI technologies may impact consumers including any potential benefits and risks that these emerging technologies may create, and ask what next steps we should take to ensure that the Commission can fulfill its statutory obligation under the TCPA to protect consumers from unwanted and often illegal robocalls and robotexts. We believe this inquiry is necessary to better understand and prepare for changes in calling and texting practices that may result from new AI-influenced technologies.

A. Artificial Intelligence – Defined For TCPA Purposes

7. We seek comment on whether, and if so how, we should define "Artificial Intelligence" for purposes of our inquiry including the particular uses of AI technologies that are relevant to fulfilling the Commission's statutory responsibilities under the TCPA. In general, AI technologies can include any program which emulates any aspect of human intelligence, such as a human voice. As a result, the term AI can encompass a wide range of technologies and functions that may extend beyond the scope of this proceeding.[13] We seek to more precisely define that term as it would bear on the Commission's responsibilities under the TCPA.

8. AI has a lengthy history that dates back for many decades.[14] Various organizations have defined AI. More recently, for example, the National Defense Authorization Act of 2019 provides several definitions of AI including "[a]n artificial system designed to think or act like a human, including cognitive architectures and neural networks."[15] The National Artificial Intelligence Initiative Act of 2020

---

[13] *See, e.g.*, National Conference of State Legislatures, *Artificial Intelligence Legislation 2023*, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation (noting that "companies are developing AI to help consumers run their homes and allow the elderly to stay in their homes longer. AI is used in health care technologies, self-driving cars, digital assistants and many other areas of daily life") (last visited Aug. 21, 2023).

[14] *See e.g.*, Rockwell Anyoha, *The History of Artificial Intelligence* (Aug. 28, 2017), https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/; Dartmouth University, *Artificial Intelligence Coined at Dartmouth 1956* https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth (last visited Sept. 26, 2023).

[15] *See* John S. McCain National Defense Authorization for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 1695 (Aug. 13, 2018) 10 U.S.C. § 2358; *see also* Advancing American AI Act § 7223(3), Pub. L. No. 117-263, 136 Stat. 2395, 3669 (Dec. 23, 2022), 40 U.S.C. § 11301. The term "artificial intelligence" is defined as the following:

> (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
>
> (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
>
> (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
>
> (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(continued….)

defines AI as "a machine-based system that can for a given set of human-defined objectives, make predictions, recommendations, or decisions."[16] The National Institute of Standards and Technology (NIST) defines AI as "the capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement."[17] The European Union has defined AI technologies as "software that is developed with one or more of the techniques and approaches . . . for a given set of human-defined objectives, [and that] generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[18] The Kansas Office of Information Technology Services recently defined "Generative artificial intelligence" as "advanced technologies such as predictive algorithms, machine learning, and large language models to process natural language and produce content in the form of text, images, or other types of media."[19] An executive order from the governor of Pennsylvania defines generative AI as "technology or tools that use predictive algorithms to create new content including audio, code, images, text, simulations, and videos."[20]

9. The Commission's authority under the TCPA encompasses current uses of AI in robocalling and robotexting as we understand them, e.g., emulating human speech and interacting with consumers as though they were live human callers when generating voice and text messages. We seek comment on whether one or more of the above examples provides a basis to define AI technologies as used in the context of making robocalls and robotexts in a manner that is consistent with the TCPA's consumer protections.

10. Are there any other definitions that we should consider for this purpose? Do specific AI technologies provide some insight as to how to define the term AI in the context of the TCPA? Voice cloning, for example, is a type of generative AI technology which attempts to emulate a human voice to generate speech using a recording of that voice.[21] "Large Language Models" seek to interpret and generate speech with the same level of proficiency as a human.[22] In particular, does the ability of AI technologies to emulate a human voice and interact with consumers through telephone calls and text messages as though they were a live person provide a basis to define these technologies under the TCPA?

11. As discussed further below, AI technologies may also enhance the analytics that allow consumers and networks to detect and block unwanted and fraudulent calls and text messages via AI generated algorithms and software. Should that factor into the definition of AI technologies in this

---

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

[16] *See* National Artificial Intelligence Initiative Act of 2020. Pub. L. 116-283 (2020) (codified at 15 U.S.C. § 9401(3)).

[17] National Institute of Standards and Technology, *Computer Security Resource Center* https://csrc.nist.gov/Topics/technologies/artificial-intelligence (last visited Aug. 15, 2023) (citing ANSI INCITS 172-220 https://www.incits.org/html/ext/ANSDIT/a3.htm (R2007)).

[18] European Union Artificial Intelligence Act, Title I Art. 3(1).

[19] *See* Kansas Office of Information Technology Services, Generative Artificial Intelligence Policy, https://governor.kansas.gov/wp-content/uploads/2023/08/P8200.00-Generative-Artificial-Intelligence-Signed.pdf (July 25, 2023) (noting that "[g]enerated content is typically remarkably similar to what a human creator might produce, such as text consisting of entire narratives of naturally reading sentences").

[20] *See* Executive Order 2023-19, Expanding and Governing the Use of Generative Artificial Intelligence Technologies Within the Commonwealth of Pennsylvania, https://www.governor.pa.gov/wp-content/uploads/2023/09/20230920_EO-2023-19_AI_Final_Executed.pdf (Sept. 20, 2023).

[21] *See, e.g.*, Anisha Kohli, *From Scams to Music, AI Voice Cloning is on the Rise* (Apr. 29, 2023) https://time.com/6275794/ai-voice-cloning-scams-music/.

[22] *See* Mariusz Flasiński, Introduction to Artificial Intelligence 229 (2016).

context? AI technologies can provide important access to individuals with disabilities or speech limitations. Are there accessibility considerations that the Commission should be aware of in defining AI technologies in this context to avoid discouraging the development of such beneficial AI tools? Should any such definition take into consideration whether the AI technology is being used for some malicious purpose such as to defraud, cause harm or wrongly obtain anything of value?[23]

12. As discussed above, the TCPA's existing prohibition on "artificial" voice messages encompasses current AI technologies that generate human voices. We note, for example, that the Commission addressed "soundboard technology" which was described as allowing a live agent to interact with consumers via the use of prerecorded voice messages selected by the agent monitoring the call.[24] In relevant part, the Soundboard petitioners argued that soundboard technology produces the functional equivalent of a conversation between the consumer and another human rather than the use of an artificial or prerecorded voice message. In rejecting that argument, the Commission noted that the "TCPA does not carve such functional equivalents out from its dictates" and determined that petitioners had not demonstrated that the technology at issue performed in the same manner as a live agent in interacting with consumers.[25]

13. Nevertheless, would it be helpful to define AI technologies in a more specific way to take into consideration the potential ability of AI technologies to function as the equivalent to a live agent when interacting with consumers? Can and should generative AI technologies be defined in ways that differ from existing technologies such as Interactive Voice Response (IVR) systems that can use artificial or prerecorded voice messages to communicate with consumers without the presence of a live agent? In addition, the TCPA defines and regulates the use of "automatic telephone dialing systems."[26] Can AI technologies function in a way that qualifies as an autodialer under the TCPA's definition? If so, should that factor into how we define any such technology? We seek comment on these and any other issues that will assist us in understanding whether and how it might be useful to define AI technologies in the context of the regulatory framework that governs robocalls and robotexts under the TCPA.

B. Benefits and Risks of AI Technologies Used to Make Robocalls and Robotexts

14. We seek information on how AI technologies may impact consumers who receive robocalls and robotexts including any potential benefits and risks that these emerging technologies may create. In seeking comment, we recognize the need to understand how these technologies may alter the functioning of the existing regulatory framework so that we may formulate policies that benefit consumers by ensuring that they continue to receive the privacy protections afforded under the TCPA from unwanted and illegal robocalls and robotexts.

15. *Benefits*. We seek comment on how AI technologies may be used to protect consumers from unwanted and illegal robocalls and robotexts. Specifically, we seek comment on how AI technologies can be used to target information to specific groups of consumers, protect consumers from unwanted robocalls and robotexts, improve the agency's ability to enforce the TCPA, and promote accessibility to individuals with disabilities. For example, are there ways that AI technologies can be used to tailor messages to individual recipients in ways that they will find more useful but that are consistent with the consumer protections afforded by the TCPA? Can AI technologies also benefit the

[23] Under the Truth-in-Caller ID Act, the Commission's rules prohibit anyone from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value. *See* 47 CFR § 64.1604(a).

[24] *See Rules and Regulations Implementing the Telephone Protection Act of 1991, NorthStar Alarm Services LLC's Petition for Expedited Declaratory Ruling, Yodel Technologies Petition for Expedited Declaratory Ruling or in the Alternative Retroactive Waiver*, CG Docket No. 02-278, Declaratory Ruling and Order, 35 FCC Rcd 14640 (2020).

[25] *Id*. at 14654, para. 16.

[26] *See* 47 U.S.C. § 227(a)(1) (defining an autodialer as "equipment which has the capacity – (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers").

calling party by enabling them to target demographics that are most interested in the subject matter of the communication? We note that some platforms already incorporate algorithms in their call blocking services by identifying patterns of robocalls across a network as well as analyzing the content of robocalls using natural language processing technology.[27] By analyzing the content of such calls, AI technology may assist consumers in recognizing scam calls or other types of calls that they do not wish to receive, thereby allowing consumers to block such calls before they reach the consumer.[28] Are there independent resources or means available to substantiate claims made by AI-based companies regarding any alleged benefits of specific AI technologies to ensure they function as described?

16. Does AI technology have the potential to improve the ability of consumers and networks to detect unwanted or fraudulent traffic and block any such communication before it reaches the consumer?[29] Would this help to restore consumer confidence in the telephone network that has been eroded by the large number of unwanted and fraudulent calls and messages? Do AI technologies also have the potential to reduce burdens associated with TCPA compliance measures? If so, might this provide an opportunity to adopt enhanced measures to better protect consumers from unwanted calls and texts? To what extent are voice service providers and third-party analytics companies already making use of AI to accomplish this?[30] To the extent that these blocking services analyze call content, are there any privacy concerns we should be aware of and, if so, how should we address those concerns? For example, we seek comment on how the use of AI technologies in this manner, whether by the provider itself or by a third party analytics company, could implicate statutory privacy regimes such as the Electronic Communications Privacy Act (ECPA),[31] section 222 of the Communications Act,[32] section 705 of the

[27] *See, e.g.*, YouMail, *The Role of Artificial Intelligence in Combatting Robocalls* (April 17, 2023) https://blog.youmail.com/2023/04/the-role-of-artificial-intelligence-in-combating-robocalls/#1. Many voice service providers make use of analytics to identify, label, and potentially block unwanted and illegal calls. *See generally* FCC, Call Blocking Tools Available to Consumers: Second Report on Call Blocking, CG Docket No. 17-59 (2021), https://docs.fcc.gov/public/attachments/DA-21-772A1_Rcd.pdf.

[28] *See, e.g.*, Remarks of FCC Chairwoman Jessica Rosenworcel, "The Opportunities and Challenges of Artificial Intelligence for Communications Networks and Consumers" ("AI has tremendous potential to expand and refine the analytics tools we have to block unwanted robocalls and robotexts. It could help restore trust in our networks. Because using these systems we can enhance our ability to see fraudulent traffic before it reaches you and stop it in its tracks.") (July 13, 2023) https://docs.fcc.gov/public/attachments/DOC-395095A1.pdf.

[29] As noted below, we also seek comment on the potential of AI technologies to block legitimate calls that the consumer might wish to receive.

[30] The Commission is aware of, and has encouraged, voice service providers' use of "reasonable analytics" for blocking, but here we are particularly interested in how AI utilizes those analytics or other tools. *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4884-88, paras. 26-35 (2019); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7625-27, paras. 25-34 (2020); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15211, 15234-38, paras. 39-47 (2020).

[31] ECPA generally prohibits a provider of "electronic communication service" from disclosing the contents of any communication carried on that service, subject to certain exceptions, such "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(a), (c)(3).

[32] For example, carriers must "protect the confidentiality of proprietary information of, and relating to, . . . customers" under section 222(a), and section 222(c) imposes additional restrictions in the case of customer proprietary network information. 47 U.S.C. § 222(a), (c).

Communications Act,[33] and section 631 of the Cable Communications Policy Act of 1984 (Cable Act),[34] which limit the extent to which providers may disclose information about subscribers. Is AI technology also useful in improving content-neutral analytics?

17. In addition, does AI technology have the potential to assist callers in ensuring they are in compliance with the various regulatory requirements under the TCPA and delivering to consumers more complete and accurate information from callers? For example, is there a potential for emerging AI technology to improve the ability of callers to respond to inquiries from consumers, ensure that only parties who have provided consent to the called party are called, process do-not-call requests, keep track of any numerical limits on calls to specific telephone numbers, and avoid calling any emergency lines or wireless telephone numbers when prohibited under the TCPA? How might the Commission confirm and measure the provision of such benefits? In 1991, when Congress enacted the TCPA, it concluded that artificial and prerecorded voice messages constituted a greater nuisance to consumers than calls with live persons. We seek comment on whether AI technology can minimize the nuisances associated with the use of artificial or prerecorded voice messages by acting as the functional equivalent to calls with live agents. For example, AI technologies have the potential to interact with consumers allowing for such technologies to be responsive to questions and process requests to stop calling. To what extent are any such benefits offset by AI technology potentially allowing callers to place even higher volumes of unwanted robocalls and robotexts?

18. We seek comment on whether AI technologies may improve the ability of persons with disabilities to communicate with a called party. For example, might AI be useful in ensuring that persons with disabilities are better able to exercise their right to revoke consent to future calls and messages? Could AI work effectively with telecommunications relay services (TRS)? For example, could it do so by allowing a TRS Communications Assistant (CA) to pause the contents of an AI-generated automated call until the CA successfully connects with the intended TRS user?[35] We further seek comment on how AI systems, either currently in use or in development, relate to accessibility tools that may generate or translate speech. These tools can provide important access to individuals with disabilities or speech limitations, and generally require direct human input. If so, are there ways to implement the TCPA's consumer privacy protections in ways that do not deter the development of such beneficial uses of AI technologies? Are there other potential benefits to consumers that will ensure better compliance with the TCPA's consumer protections? In addition, are there ways that the Commission can utilize AI technologies to improve our ability to monitor and enforce compliance with our TCPA-related rules? If so, how? Are there any current examples of how AI technologies are being used for these beneficial purposes? We seek comment on these and any other potential benefits of AI technology in the context of this inquiry.

19. *Risks*. We also seek comment on ways that AI is used or potentially could be used to make illegal, fraudulent, or otherwise unwanted robocalls and robotexts. For example, can bad actors use

[33] Section 705(a) generally prohibits unauthorized parties from receiving or intercepting communications and using or disclosing such communications. 47 U.S.C. § 605(a).

[34] Among other things, section 631 prohibits any cable operator from disclosing "personally identifiable information" without the prior consent of the subscriber. 47 U.S.C. § 551(c)(1).

[35] *See, e.g.*, Letter from Christian Vogler, Technology Access Program, Rehabilitation Engineering Research Center on Technology for the Deaf and Hard of Hearing, Gallaudet University, to Marlene Dortch, FCC, CG Docket Nos. 10-51 and 03-123, Attach. at 26, 57 (filed July 5, 2017) https://www.fcc.gov/ecfs/document/10705144575070/2 (VRS Survey Public Results noting prerecorded messages begin before interpreter answers the receiving call). Consumer complaints filed with the Commission also detail issues with automated calls being inaccessible to TRS users since the automated message plays as soon as the TRS call agent answers the call but before the intended TRS user is connected, resulting in loss of content and missed options for the TRS user before the automated call terminates itself. An example is a reminder of a medical appointment with options to confirm or cancel the appointment.

AI technologies to avoid detection by analytic systems designed to protect consumers by blocking certain types of calls? Is there a risk that AI technologies might be used in such a way as to inadvertently block legitimate calls and messages? If so, are there steps the Commission or industry could take to prevent this? Does AI technology reduce the potential costs to make or send high volumes of robocalls and robotexts by eliminating the need to hire and train any human agents? Would AI technology add to the costs of those industry stakeholders proactively attempting to detect and reduce high volumes of robocalls and robotexts in their networks? Should the Commission be concerned about these potential harms?

20. Is there a risk that AI technology can be used in ways to make the public more susceptible to fraudulent calls by appearing to be from someone the consumer knows or trusts, or otherwise tailored to convince the recipient that the call is from a legitimate source? Similarly, is there a risk that increased use of AI could make it easier for bad actors to place a higher volume of calls that appear to be from a real person, making call recipients more likely to trust the caller? For example, are bad actors cloning the voices of specific persons to persuade consumers of call legitimacy-and will bad actors do so with increasing frequency and impact as the quality of voice cloning increases and the cost decreases?[36] What is the effect? As discussed below, should the Commission consider ways to verify the authenticity of legitimately generated AI voice or text content from trusted sources, such as through the use of watermarks, certificates, labels, signatures or other forms of labels? Is there a potential for AI technologies to be used in ways that defraud consumers, introduce harmful bias, disrupt elections, perpetuate the commission of crimes, or induce widespread panic such as by making false emergency robocalls mimicking the voices of public officials or other trusted sources in ways that violate the TCPA or other consumer protection statutes?[37]

21. Are there current examples of how AI technologies are used in such disruptive ways that might inform our future policy decisions as we attempt to protect the public from such callers via our authority under the TCPA and Communications Act? Are there any examples of AI being used to generate content for robocalls and text messages and to make calls and send messages for the purpose discussed above? What are the risks of such calls? Is the use of this technology particularly pernicious such that we should treat AI-assisted robocalls and robotexts differently than traditional robocalls and robotexts? Are there any benefits of using AI technology in this way that we should seek to preserve or encourage?

22. As noted above, unwanted calls and text messages are already the top source of consumer complaints with the Commission. By some estimates, consumers are scammed by fraudulent robocalls that cost them billions of dollars each year.[38] Does AI technology have the potential to make these unwanted and often fraudulent communications more effective by targeting specific demographics that are more susceptible to scams, such as the elderly? Similarly, does the use of AI technology have the potential to increase the risk of unwanted and fraudulent calls and texts to individuals for whom English

[36] *See, e.g.*, Federal Trade Commission, *Scammers Use AI to Enhance Their Family Emergency Schemes*, Consumer Alert (Mar. 20, 2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes ("All [a scammer] needs is a short audio clip of your family member's voice—which he [or she] could get from content posted online—and a voice-cloning program."); Joe Hernandez, *That Panicky Call from a Relative? It Could Be a Thief Using a Voice Clone, FTC Warns*, NPR Technology (Mar. 22, 2023), https://www.npr.org/2023/03/22/1165448073/voice-clones-ai-scams-ftc.

[37] *See, e.g.*, See Faith Karimi, *'Mom, these bad men have me.': She believes scammers cloned her voice in a fake kidnapping* (April 29, 2023), https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html; Keep Your AI Claims in Check, FTC Business Blog, https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check (Feb. 27, 2023); Michael Atleson, Chatbots, Deepfakes, and Voice Clones: AI Deception for Sale, FTC Business Blog, March 20, 2023, https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale (Mar. 20, 2023).

[38] Yudhijit Bhathacharee, *Who's Making All These Scam Calls?* (Jan. 27, 2021) (estimating that Americans lose from $3.5 billion to $20 billion every year from fraudulent call scams): https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html.

is a second language? Is there evidence that the use of generative AI technology has already increased the number of unwanted calls and text messages?

23. Are there potential negative consequences for other consumer protection statutes enforced under the Commission's rules such as the CAN-SPAM Act which protects consumers from unwanted mobile service electronic mail messages?[39] Are there other potential negative consequences to consumers from AI technologies that will allow callers to evade the TCPA's consumer protections? What is the estimated timeframe before AI technologies begin to have a substantial impact on the TCPA and other consumer protections?

C. Future Steps to Address AI Technologies

24. We seek comment on what steps, if any, the Commission should consider to further this inquiry. As noted above, the TCPA specifically authorizes the Commission to make "technical and procedural standards for systems that are used to transmit any artificial or prerecorded voice message via telephone."[40] In addition, the legislative history contemplated the Commission's need for the flexibility to address future technologies that impact the TCPA's consumer privacy protections from unwanted robocalls.[41] The TCPA also prohibits the use of an "artificial" voice message in calls to a residential or wireless telephone number absent the prior express consent of the called party or a recognized exemption.[42] Is there any reason to conclude that these existing legal authorities do not provide the Commission with sufficient statutory authority to ensure that the use of emerging AI technologies does not erode consumer protections under the TCPA or other consumer protection statutes when used to communicate via robocall or robotexts? Are there consumer education or outreach initiatives that the Commission could conduct to raise awareness of the risks posed by emerging AI technologies including the targeting of elderly and non-English speaking populations?

25. We believe that certain AI technologies such as "voice cloning" appear to fall within the TCPA's existing prohibition on artificial or prerecorded voice messages because this technology artificially simulates a human voice. We seek comment on whether it is necessary or even possible to determine at this point whether future types of current AI technologies fall within the TCPA's existing prohibitions on artificial or prerecorded voice messages. As noted above, "voice cloning" and other similar technologies involve emulating human voices for telephone calls to consumers, but such calls may not involve actual direct interaction with a live person. What factors, if any, other than the participation of a live person on the call should we take into consideration in reaching any conclusions? For example, should we consider the extent to which such technology provides the functional equivalent to interacting with a live person? What factors would be included in any such analysis to determine if a particular technology is providing the functional equivalent of an interaction with a live person? Should, or may, we consider the character of the voice clone—*e.g.*, a clone of a call recipient's personal contact, a public official, a celebrity, etc.—as relevant to our analyses under the TCPA? To what extent does the potential liability for substantial regulatory fines and private rights of action encourage AI user compliance with the TCPA's consumer protections?[43]

26. Alternatively, as the Commission suggested in the Soundboard ruling, does the TCPA not allow any carve out for functional equivalency of a live person for any technology if the call uses an artificial or prerecorded voice? Should voice alteration technologies that can alter a live speaker's voice

[39] *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (*CAN-SPAM Act*), *codified at* 15 U.S.C. § 7701-7713, 18 U.S.C. 1037 and 28 U.S.C. § 994. *See also* 47 CFR § 64.3100.

[40] *See* 47 U.S.C. § 227(d)(3).

[41] 137 Cong. Rec. S18784 (1991) (statement of Sen. Hollings) ("The FCC is given the flexibility to consider what rules should apply to future technologies as well as existing technologies").

[42] *See* 47 U.S.C. § 227(b)(1).

[43] *See* 47 U.S.C. § 227(b)(3) (authorizing private rights of action for TCPA violations); 47 CFR § 1.80.

using AI so that it sounds like a different person always constitute an artificial or prerecorded voice under the TCPA? What factors should we consider in that context? For example, are there steps we can take to ensure that important accessibility tools for individuals with disabilities are not negatively impacted? Are there additional steps to take to ensure the accessibility of such automated calls?[44]

27. How would consumers ever realize that they are interacting with an AI generated voice if such technology becomes functionally equivalent to a human? Should the Commission require "digital watermarks" that can indicate whether a voice on a robocall is generated by AI?[45] Could the Commission use its authority under section 227(d)(3), or any other authority, to require the use of such watermarks? Should the Commission require callers that are using AI technologies that emulate a human voice to make that disclosure on the call? We note that the TCPA requires that all artificial or prerecorded voice messages must at the beginning of the message state the identity of the party initiating the call.[46] Should this disclosure include an additional declaration that AI technologies are being used on the call? Similarly, should we require AI-generated robocalls to include a specific contact for complaints about factually false or otherwise unlawful AI-generated communications?[47] Could and should the developers of AI technology and not just the robocallers using that technology be held accountable if their systems are designed to operate in a way that is inconsistent with the TCPA or other related consumer protection statutes, or do not contain adequate safeguards to prevent them from being used in illegal ways?[48] Are there specific issues or measures that we should consider to ensure that the TCPA's protections afforded to emergency lines including 911 lines, any emergency line of a hospital, medical physician, health care facility, poison control center, or fire protection or law enforcement agency are not undermined by AI technologies?[49]

28. What other steps can we take to identify the root causes of AI-driven robocall or robotext scams? For example, should we solicit information from industry regarding the type of AI technologies used in particular scams, either on a regular basis or in connection with investigations? Should we inquire as to whether the AI technology used was developed for general legal uses, and misused, or whether it was purpose-built for unlawful applications? If the AI technology was developed for general use, were there safeguards in place to ensure it was not misused? If so, how were they disabled? And how best can we share the information that we gather about fraudulent uses of AI within our purview with our sister agencies, who are charged with addressing malicious uses of AI in other contexts?

29. Further to that point, we seek comment on what steps the Commission might take with respect to third parties to further this inquiry. How might we consider ongoing means to stay informed of relevant emerging AI technologies? For example, should we consider a joint effort with other federal and state agencies, universities, and private industry entities to remain informed of emerging AI technologies and related practices that might impact consumer protections from unwanted and illegal robocalls and

---

[44] *See supra* para. 18.

[45] Digital watermarks can be inserted in various digital data such as audio or images allowing authentication of the data. *See, e.g.*, Bill Rosenblatt, *Google and OpenAI Plan Technology to Track AI-Generated Content* (July 22, 2023), Google And OpenAI Plan Technology To Track AI-Generated Content (forbes.com); Digital Watermarking. https://www.sciencedirect.com/topics/engineering/digital-watermarking.

[46] *See* 47 U.S.C. § 227(d)(3)(A).

[47] *Id.*

[48] The Commission has clarified that an entity may be found to have made or initiated a call under the TCPA in one of two ways: first, by "tak[ing] the steps necessary to physically place a telephone call"; and second, by being "so involved in the placing of a specific telephone call as to be directly liable for initiating it." *See DISH Declaratory Ruling*, 28 FCC Rcd at 6583, paras. 26-27 (2013).

[49] *See* 47 U.S.C. § 227(b)(1)(A)(i); *see also* 47 CFR § 64.1202 (affording protections to Public Safety Answering Points (PSAP) from non-emergency robocalls).

robotext schemes?[50] What have other federal and state agencies done to address the use of AI systems that might be relevant to this inquiry?[51] Are there ways that the Commission might facilitate voluntary compliance with the TCPA through the cooperation of AI developers to ensure that they are aware of these obligations and can direct their development process in ways that are consistent with the TCPA, and contain safeguards to protect against uses violative of the TCPA?[52] If so, what is the best way to facilitate these voluntary efforts? We seek comment on these and any other next steps that would further the objectives of this inquiry.

IV. PROCEDURAL MATTERS

30. *Ex Parte Rules*. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[53] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filing in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable.pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

31. *Comment Filing Procedures*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by paper. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Electronic Filers: Comments may be filed electronically by accessing ECFS at https://www.fcc.gov/ecfs.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.
    - Effective March 19, 2020, and until further notice, the Commission no longer accepts any

[50] We note that the Technical Advisory Council (TAC) provides technical advice to the Commission, https://www.fcc.gov/general/technological-advisory-council.

[51] *See, e.g.*, Claudia Grisales, *Schumer meets with bipartisan group of senators to build a coalition for AI law* (May 18, 2023) https://www.npr.org/2023/05/18/1176894731/schumer-meets-with-bipartisan-group-of-senators-to-build-a-coalition-for-ai-law.

[52] *See, e.g.*, Serena Marshall, *Tech giants commit to Biden administration-brokered AI safety rules* (July 21, 2023) https://www.abc15.com/tech-giants-commit-to-biden-administration-brokered-ai-safety-rules.

[53] 47 CFR §§ 1.1200 *et seq*. *See* 47 CFR § 1.1200(a) ("Where the public interest so requires in a particular proceeding, the Commission and its staff retain the discretion to modify the applicable *ex parte* rules by order, letter, or public notice").

hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19.[54]

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, D.C. 20554.

32. *Availability of Documents*. Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. These documents will also be available for public inspection during regular business hours in the FCC Reference Information Center, Federal Communications Commission, 45 L Street NE, Washington, D.C. 20554.

33. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

34. *Further Information*. For additional information on this proceeding, contact Richard D. Smith of the Consumer and Governmental Affairs Bureau, at Richard.Smith@fcc.gov or (717) 338-2797.

V. ORDERING CLAUSES

35. Accordingly, IT IS ORDERED that, pursuant to sections 1-4, 227, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 227, and 403, this Notice of Inquiry IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[54] *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, Notice of Inquiry (November 15, 2023)

If Tom Hanks called, I would pick up the phone. If he spoke in a familiar way during that call, I would definitely listen. To be clear, the star of Big and Saving Private Ryan is not dialing me anytime soon. But a video using his voice is on the internet hawking dental plans. None of this is happening with his permission. This is happening because scam artists are playing with artificial intelligence and testing our ability to separate vocal fact from fiction in order to commit fraud.

Now imagine instead a call from a friend or family member. Of course you pick up. But maybe that voice sounds off and something feels wrong. Maybe it is because the individual you think is on the other end of the line is telling you about an imminent emergency and pleading with you to send money. Like the hard sell from Tom Hanks, it is also a scam. Because you are not actually talking to who you think you are, you are speaking with a con artist using artificial intelligence to clone the voice of someone you know.

If this future sounds far off, think again. We see on the internet how fraudsters are already playing with this technology. We know that scam artists want to explore ways to use this technology over the phone.

I recently had the opportunity to sit down with AARP and talk about what the combination of unwanted robocalls and robotexts and artificial intelligence will mean for consumers. I learned about how voice cloning scams are growing and how they can cause special harm for older adults. Imagine, for instance, a grandparent fearing they will get a call from their grandchild, only to learn it was fraudster on the other end of the line, preying on their willingness to forward money to family.

The anxiety about these technology developments is real. Rightfully so. But I think we make a mistake if we only focus on the potential for harm. We need to equally focus on how artificial intelligence can radically improve the tools we have today to block unwanted robocalls and robotexts. We are talking about technology that can see patterns in our network traffic unlike anything we have today. This can lead to the development of analytic tools that are exponentially better at finding fraud before it ever reaches us at home. Used at scale, we can not only stop this junk, we can help restore trust in our networks.

That is why today we are launching an inquiry to ask how artificial intelligence is being used right now to recognize patterns in our network traffic and how they could be used in the future. We know the risks that this technology involves, but we also want to harness the benefits—just like the recently released Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence recommends.

That is not to say this will be easy. Like Tom Hanks said as the ragtag coach Jimmy Dugan in A League of Their Own, "the hard . . . is what makes it great." We have work to do to harness artificial intelligence for good. But I am an optimist and I believe this is possible. So let's get to it. Let's see how we can use artificial intelligence to get this junk off the line.

I want to thank the staff responsible for our efforts today, including Jerusha Burnett, Zac Champ, Aaron Garza, Josh Mendelsohn, Michael Scott, Suzy Rosen Singleton, Richard Smith, Mark Stone, Kristi Thornton, and George Phelan from the Consumer and Governmental Affairs Bureau; Kristi Thompson from the Enforcement Bureau; Richard Mallen, Marcus Maher, Michele Ellison, Jeff Steinberg, Royce Sherlock, and Wade Lindsay from the Office of General Counsel; Michelle Schaefer and Andrew Wise from the Office of Economics and Analytics; Martin Doczkat and Dana Shaffer from the Office of Engineering and Technology; Michael Antonino, Maureen Bizhko, Kenneth Carlberg, Shawn Cochran, Gerald English, John Evanoff, David Furth, David Sieradzki, Austin Randazzo, and James Wiley from

the Public Safety and Homeland Security Bureau; Jonathan Lechter from the Wireline Competition Bureau; and Arpan Sura and Paul Powell from the Wireless Telecommunications Bureau.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, Notice of Inquiry (November 15, 2023)

Over the last few months, I've been proud to see our government convene quickly and effectively to explore the implications of artificial intelligence ("AI"). Congress is deeply engaged on this issue, convening hearings and introducing bills on the implications of AI for sectors from healthcare to homeland security. The White House is as well, with President Biden issuing a landmark executive order ("EO") aimed at seizing the promise and managing the risks of AI for the American people. Our miliary is engaged. Our scientists are engaged. And so are our agencies.

This intersectionality is critical. Because while the future of AI remains uncertain, one thing is clear: it has the potential to impact, if not transform, nearly every aspect of American life. Because of that potential, each part of our government bears a responsibility to better understand the risks and opportunities presented within its mandate, while being mindful of the limits of its experience and its authority. And in this era of rapid technological change, we must collaborate, lending our learnings and sharing our expertise across agencies to better serve our citizens and consumers.

That is what the Biden EO charges us with doing, and what the Chairwoman has done by circulating the item before us today.

Specifically, the EO charges the FCC with examining the impact of AI on unwanted robocalls and robotexts. As the EO – and today's notice of inquiry ("NOI") – acknowledges, AI holds both promise and risk when it comes to our ongoing efforts against spam calls. AI technologies can be leveraged to block unwanted robocalls and robotexts. In fact, wireless carriers use various algorithms for this purpose today, and we ask them for more information about that usage in the NOI. But AI can also facilitate or exacerbate spam – and scam – calls.

The clearest example of this to date is voice cloning – generative AI technology that uses a recording of a human voice to generate speech sounding like that voice. In one recent news story, a mom in Arizona believes bad actors cloned her daughter's voice in what was ultimately a fake kidnapping phone scam.[1] White House Deputy Chief of Staff Bruce Reed, charged with developing the administration's AI strategy, says "[v]oice cloning is one thing that keeps me up at night."[2] The NOI asks about the frequency and impact of voice cloning in robotexts and robocalls, and how the Commission might address it, such as by verifying the authenticity of legitimately-generated AI voice or text content from trusted sources.

Of course, voice cloning is an already-known issue, and one that falls within our existing statutory authority (i.e., the Telephone Consumer Protection Act's ("TCPA") prohibition on calls using artificial or prerecorded voices without consent).[3] AI is a powerful, and evolving, technology. We do not know all of the issues that it may trigger – or all the benefits it may hold. So this item seeks to explore and find out. It poses some questions that will be best answered by our regulatees, such as whether AI technology can be used to reduce burdens associated with TCPA compliance measures, and how AI can work effectively within telecommunications relay services. But it also seeks information from AI developers and others who may be less familiar with our regulations, yet may still find themselves within them. For example, the NOI asks how the FCC might cooperate with AI developers to ensure they are aware of the TCPA's obligations so they can develop their products in ways consistent with the statute, and with safeguards in place to

[1] *See* Faith Karimi, "'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping," CNN (Apr. 29, 2023), https://www.cnn.com/2023/04/29/us/ai-scam-calls-kidnapping-cec/index.html.

[2] Nancy Scola, "Biden's Elusive AI Whisperer Finally Goes on the Record. Here's His Warning." Politico (Nov. 2, 2023), https://www.politico.com/news/magazine/2023/11/02/bruce-reed-ai-biden-tech-00124375.

[3] *See* 47 U.S.C. § 227(b)(1)(A)-(B).

protect against bad actors using their products in ways violative of the TCPA.

I want to thank my colleagues for agreeing to my additions to the item. At a time when scammers can use tools like WormGPT and FraudGPT to facilitate their crimes,[4] it is critical that the FCC use its enforcement authority to identify what we can about the root causes of AI-driven robocall and robotext scams, and share that information with our sister agencies charged with addressing malicious uses of AI within their domains. Under the Chairwoman's leadership, our anti-robocall work has been characterized by coordination and cooperation, including with state attorneys general and the Industry Traceback Group. I see this collaboration as following in that same vein, and hope it will be similarly successful.

I also want to thank the FCC staff who worked on this item – you are a key part of this whole-of-government effort around AI, and this item has my full support.

[4] *See, e.g.* Matt Burgess, "Criminals Have Created Their Own ChatGPT Clones," WIRED (Aug. 7, 2023), https://www.wired.com/story/chatgpt-scams-fraudgpt-wormgpt-crime/; Michael Kan, "After WormGPT, FraudGPT Emerges to Help Scammers Steal Your Data," PCMag (July 25, 2023), https://www.pcmag.com/news/after-wormgpt-fraudgpt-emerges-to-help-scammers-steal-your-data.