Before the
Federal Communications Commission
Washington, DC 20554

In the matter of: Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts	CG Docket No. 23-362 FCC 23-101

To: The Federal Communications Commission

Date: July 29, 2024

Comment of the Federal Trade Commission

I. Introduction

On November 15, 2023, the FCC issued a Notice of Inquiry through which the FCC sought to "better understand the implications of emerging artificial intelligence (AI) technologies as part of … ongoing efforts to protect consumers from unwanted and illegal telephone calls and text messages under the Telephone Consumer Protection Act."[1] Among other questions, the Notice of Inquiry asked: "What have other federal and state agencies done to address the use of AI systems that might be relevant to this inquiry?" In partial answer to that question, the FTC submits this summary of the FTC's recent Voice Cloning Challenge.

II. Interest and Experience of the Federal Trade Commission

The FTC, the nation's consumer protection agency, is an independent agency that works to protect the American public from unfair or deceptive business practices. While primarily a law enforcement agency, the FTC uses a variety of other tools to fulfill its mission,

[1] Fed. Commc'ns Comm'n, FCC 23-101, Notice of Inquiry, In the matter of: Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, CG Docket No. 23-362, at 1 (Nov. 15, 2023) (hereinafter "NOI").

including rulemaking, research, studies, public outreach and engagement, and consumer and business education. The FTC is bringing all of these tools to bear in addressing the rapid emergence of new technology powered by AI, including voice cloning. AI presents opportunities for consumers, our economy, and our society. But it also poses significant risks, and the Commission is working to address these risks in a number of ways, while also promoting innovation that affirms America's leadership around this emerging technology. The FTC has consistently worked to send a clear and unequivocal message to industry that there is no AI exception to consumer protection or antitrust laws.

The Commission is using its existing legal authorities to take action against illegal practices involving AI. For instance, the FTC alleged that Amazon and Ring used highly private data—voice recordings collected by Amazon's Alexa voice assistant[2] and videos collected by Ring's internet-connected home security cameras[3]—to train their algorithms while violating customers' privacy. The Alexa matter, in particular, underscored that the prohibition in the Children's Online Privacy Protection Act Rule on the indefinite retention of children's data are not superseded by claims from businesses that data must be indefinitely retained to improve machine learning algorithms. In enforcement actions against two other companies—Automators AI[4] and WealthPress[5]—the FTC alleged that the

---

[2] Press Release, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023); Complaint, *United States v. Amazon.com, Inc.*, No. 23-cv-811 (W.D. Wash. filed May 31, 2023).

[3] Press Release, FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras (May 31, 2023); Complaint, *FTC v. Ring LLC*, No. 23-cv-1549 (D.D.C. filed May 31, 2023).

[4] Press Release, FTC Action Leads to Ban for Owners of Automators AI E-Commerce Money-Making Scheme (Feb. 27, 2024); Complaint, *FTC v. Automators LLC*, No. 23-cv-1444 (S.D. Cal. filed Aug. 8, 2023).

[5] Press Release, FTC Suit Requires Investment Advice Company WealthPress to Pay $1.7 Million for Deceiving Consumers (Jan. 13, 2023); Complaint, *FTC v. WealthPress Holdings, LLC*, No. 23-cv-46 (M.D. Fla. filed Jan. 12, 2023).

defendants engaged in investment scams and touted the use of AI to enhance their false claims of investment success.[6] And the Commission charged Rite Aid with failing to implement reasonable safeguards when the company deployed AI facial recognition technology that falsely tagged consumers, especially women and people of color, as shoplifters or other bad actors.[7]

The Commission has also issued a rule outlawing government and business impersonation scams—a type of fraud that generative AI can turbocharge.[8] The Commission has also embarked on a supplemental rulemaking proposing to extend this ban to the impersonation of individuals and to prohibit providing scammers with the means and instruments to execute such scams.[9] The Commission has also made clear that AI robocalls are not exempt from the Telemarketing Sales Rule.[10] And the Commission proposed a rule cracking down on firms that generate fake reviews—an online scourge that AI threatens to exacerbate.[11]

The Commission is also helping guide consumers and businesses as they navigate the potential perils of AI. The Commission has issued award-winning consumer and business guidance around various AI-

---

[6] *See also* Complaint, *FTC v. DK Automation LLC*, No. 22-cv-23760 (S.D. Fla. filed Nov. 16, 2022) (among other things, Defendants marketed a "Crypto Automation" package including a "secret passive income crypto trading bot" that was purportedly "a fully automated, fully-automatic algorithm" that "will trade for you 24-7 so you will generate your profits even while you sleep").

[7] Press Release, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023); Complaint, *FTC v. Rite Aid Corp.*, No. 23-cv-5023 (E.D. Pa. filed Dec. 19, 2023).

[8] Press Release, FTC Announces Impersonation Rule Goes into Effect Today (Apr. 1, 2024).

[9] *Id.*

[10] Press Release, FTC Implements New Protections for Businesses Against Telemarketing Fraud and Affirms Protections Against AI-enabled Scam Calls (Mar. 7, 2024).

[11] Press Release, Federal Trade Commission Announces Proposed Rule Banning Fake Reviews and Testimonials (Jun. 30, 2023).

related issues.[12] Moreover, the Commission held a Technology Summit concerning AI[13], a workshop devoted to the emergence of voice cloning technologies,[14] and a roundtable concerning the impact of generative AI on creative professionals.[15] Finally, the Commission wants to ensure that biometric information—a particularly sensitive category of health data—is being protected, and in 2023, issued a policy statement identifying factors the FTC will consider in determining whether business' use of biometric information or biometric information technologies, including those powered by AI and machine learning, could be unfair in violation of the FTC Act.[16]

The Commission has also tapped American ingenuity to help fight back against AI-enabled fraud through the FTC's Voice Cloning Challenge, discussed next.

III. The Voice Cloning Challenge

The FTC's Voice Cloning Challenge was an open, exploratory challenge to the public to develop multidisciplinary approaches—from

---

[12] *See* Lesley Fair, For Business Opportunity Sellers, FTC says "AI" Stands for "Allegedly Inaccurate," FTC Business Blog (Aug. 22, 2023); Michael Atleson, Can't Lose What You Never Had: Claims About Digital Ownership and Creation in the Age of Generative AI, FTC Business Blog (Aug. 16, 2023); Michael Atleson, Watching the Detectives: Suspicious Marketing Claims for Tools That Spot AI-Generated Content, FTC Business Blog (July 6, 2023); Elisa Jillson, Hey, Alexa! What Are You Doing With My Data?, FTC Business Blog (June 13, 2023); Michael Atleson, The Luring Test: AI and the Engineering of Consumer Trust, FTC Business Blog (May 1, 2023); Michael Atleson, Keep Your AI Claims in Check, FTC Business Blog (Feb. 27, 2023); Elisa Jillson, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, FTC Business Blog (Apr. 19, 2021).

[13] Press Release, FTC Hosts Virtual Tech Summit on January 25 Focused on Artificial Intelligence (Jan. 24, 2024).

[14] Event Website, You Don't Say: An FTC Workshop on Voice Cloning Technologies (Jan. 28, 2020).

[15] Press Release, FTC to Host Roundtable Discussion on October 4 on Artificial Intelligence and the Creative Fields (Oct. 3, 2023).

[16] Press Release, FTC Warns About Misuses of Biometric Information and Harm to Consumers (May 18, 2023).

products to policies to procedures—aimed at protecting consumers from AI-enabled voice cloning harms, such as fraud and the broader misuse of biometric data and creative content. Submissions that were able to address harms, as defined in the Challenge's judging criteria, were eligible for challenge prizes that could be used to further develop and implement the given solution.

The Challenge encouraged individuals, teams of individuals, for-profit legal entities and/or non-profit organizations (collectively, "Participants") to develop and submit ideas aimed at protecting consumers from AI-enabled voice cloning harms ("Submissions"). Submissions were required to, at a minimum, address one or more of the following voice cloning harm intervention points:

- Prevention or Authentication. Methods to limit the use and application of voice cloning software by unauthorized users.
- Real-time Detection or Monitoring. Methods to detect cloned voices or the use of voice cloning technology.
- Post-use Evaluation. Methods to check after the fact if audio clips contain cloned voices.

A. Background

While AI-enabled voice cloning (the creation of an artificial simulation of a person's voice) may have important beneficial applications, such as in the medical field or options for accessibility, it can also create risks of fraud and other misuse of biometric data and creative content. Scammers already are using voice cloning technology to turbocharge fraud. As publicly-available voice cloning tools proliferate, the problem will grow. Voice cloning technology can help "grandparent scammers" clone the voice of a loved one to call a family member and ask for immediate financial assistance. Scammers can also clone the voice of a company's executives to make phishing calls leading to unauthorized wire transfers.

While the marketplace has focused research on tools to identify whether text and images have been created by AI technology, there is less focus on discerning whether voices are real or synthetic. Early investigation has revealed widely varying notions about how effective voice cloning detection solutions may be. However, voice cloning itself is rapidly improving and becoming easier to use.

The FTC has undertaken significant efforts to raise awareness about risks of AI, including voice cloning. The FTC held a workshop in 2020 called "You Don't Say: An FTC Workshop on Voice Cloning Technologies." Further, staff has released numerous written pieces about aspects of that topic, including blogs and educational material for both consumers and businesses (for example: "Voice cloning: Where WOW meets OMG" and "Scammers use AI to enhance their family emergency schemes"). The Voice Cloning Challenge was the FTC's latest effort on the AI-enabled voice cloning front.

B. Challenge Execution

The Challenge was conducted pursuant to Section 105 of the America COMPETES Reauthorization Act of 2010, P.L. 111-358 (Jan. 4, 2011), codified as amended at 15 U.S.C. § 3719. Entering the Challenge required Participants' full agreement to the Challenge's Official Rules. The FTC first announced the Challenge on November 16, 2023. The Challenge was open to accept Submissions from January 2 to 12, 2024. To enter, Participants submitted a Registration Form on the Challenge website.

1. Submission Basics

Participants developed and submitted ideas that would help protect consumers from AI-enabled voice cloning harms. Submissions were required to address at least one of the three voice cloning harm intervention points mentioned above (Prevention or Authentication, Real-time Detection or Monitoring, and Post-use Evaluation). Submissions that did not address at least one of these intervention points were not be considered.

Submissions contained up to three components that described the ideas the Participants had developed to protect consumers from AI-enabled voice cloning harms:

1. Required: A title and a brief text description ("abstract") of how the Submission would function, which could be made public and should be easy for the public to understand (limited to one page).

2. Optional: A publicly accessible link to a video presentation describing and/or demonstrating how the Submission would function (limited to five minutes long). More specifically, videos were meant to: (i) state what the Submission is specifically designed to do; (ii) if possible,

demonstrate the Submission; and (iii) explain what impact the Submission would have for consumers

3. Required: A detailed written description of the Submission that would enable the Challenge Judges to evaluate how the Submission met the assessment criteria set out in the Challenge Rules (limited to 10 pages).

Any Submission that was publicly available prior to the start of the Challenge Period (November 16, 2023) was not eligible for entry in the Challenge, unless the Submission incorporated significant new functionality, features, or changes.

2. Judging Process

The Submissions were judged in two phases: the "Initial Phase" and the "Final Phase."

In the Initial Phase, submissions were screened by a qualified Internal Panel at the FTC. The Internal Panel evaluated Submissions based on the judging criteria in the Challenge Rules to select up to twenty Finalist Submissions. The Internal Panel only assessed the Participants' abstracts and videos, if submitted, without the Detailed Explanations.

In the Final Phase, Finalist Submissions were judged by an expert panel of Challenge Judges. In addition to looking at the abstracts and videos, if submitted, the Judges reviewed the Detailed Explanations. The Challenge Judges were:

- **Arvind Narayanan**, a professor of computer science at Princeton and the director of the Center for Information Technology Policy. He co-authored a textbook on fairness and machine learning and is currently co-authoring a book on AI snake oil. His work was among the first to show how machine learning reflects cultural stereotypes, and his doctoral research showed the fundamental limits of de-identification. Narayanan is a recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE).
- **Beau Woods**, a leader with the I Am The Cavalry grassroots initiative, Founder/CEO of Stratigos Security, and Cyber Safety Innovation Fellow with the Atlantic Council. His work bridges the gap between the security research and public policy communities, to ensure connected technology

that can impact life and safety is worthy of our trust. Over the past several years in this capacity, he has consulted with the healthcare, automotive, aviation, rail, and IoT industries, as well as cyber security researchers, US and international policy makers, and the White House.

- **Britt Paris**, assistant professor at the Rutgers University School of Communication & Information, and a critical informatics scholar studying the political economy of information infrastructure, as it relates to evidentiary standards and political action. She has published work on Internet infrastructure projects, artificial intelligence-generated information objects, digital labor, and civic data, analyzed through the lenses of political economy, cultural studies, and feminist social epistemology.

3. Judging Criteria

Submissions were assessed using the following Judging Criteria:

One—Administrability and Feasibility to Execute: How well does the Submission work? How feasible /administrable is it to deploy? (50 points out of 100 total score).

How well does the Submission address at least one of the voice cloning harm intervention points listed above? If the idea is currently conceptual, what is the potential of this Submission to address at least one of the points?

Are there any conditions that need to be met in the current ecosystem for the Submission to be implemented? Can it function in today's marketplace? (E.g., Does it require changes to telecommunications networks? Does it require active cooperation by voice service providers and/or telephone manufacturers?) What resources are required to execute the Submission?

How many consumers can be protected? If applicable, does it matter what type of technology consumers use—wireline vs. VoIP vs. mobile phones, different brands of phones, videoconferencing, digital voice clips? Proposals that will work for more consumers were scored higher.

Participants were also asked what evidence supported their responses to the questions above and whether there were aspects of their Submissions that required further development.

Two—Increased Company Responsibility, Reduced Consumer Burden: If implemented by upstream actors, how does the Submission place liability and responsibility on companies and minimize burden on consumers? How do we ensure that the assignment of liability and responsibility matches the resources, information, and power of the relevant actors? How does this mitigate risks at their source or otherwise strategically intervene upstream before harms occur? If required to be implemented by consumers, how easy is it for consumers to use? (20 points out of 100 total score).

Is the Submission something that upstream actors would implement to protect consumers, or is the Submission something that consumers would implement individually—or a mix of both?

For ideas that would be implemented by upstream actors: How does it place the onus on the upstream actors (e.g., voice cloning detection service providers, providers of voice cloning technology, telecommunications networks, telephone manufacturers) to mitigate harm and minimize burden on consumers? What is required of service providers to stand up and roll out the Submission? What consumer engagement is there, if any? Would the Submission be accessible to people with disabilities?

For ideas that would be implemented by consumers: How easy is the tool for everyday consumers without technical expertise to set up and use? How much of a change to a user's regular routine would it represent? Would the Submission be accessible to people with disabilities?

Participants were also asked what evidence supported their responses to the questions above and whether there were aspects of their Submissions that required further development.

Three—Resilience: How is the Submission resilient to rapid technological change and evolving business practices? How easily can it be sustained and adapted as voice cloning technology improves, including how the idea will avoid or mitigate any additional safety and security risks that it itself might introduce? (30 points out of 100 total score).

How will the Submission stay up-to-date? How easy might it be for bad actors to adapt and counter the Submission? How flexible is the Submission to adapt to new voice cloning techniques?

Participants were also asked what evidence supported their responses to the questions above, with a reminder that the real test of a system is not whether the Participant can break it (or find loopholes)—it's whether bad actors can, as well as whether there were aspects of their Submissions that required further development.

C. Challenge Winners and Prizes

On April 8, 2024, the FTC announced the outcome of the Voice Cloning Challenge: the judges selected four coequal winners of the Challenge. Three winners, from an individual and two small organizations, equally split the monetary prize pool of $35,000; the fourth winner was from a large organization (ten or more people, which were ineligible for monetary prizes).

The FTC Voice Cloning Challenge winners are:

"'**AI Detect**' for consumer and enterprise apps and devices" (Video / Abstract). Submitted by David Przygoda and Dr. Carol Espy-Wilson from the small organization OmniSpeech (located in College Park, Maryland). AI detect uses AI algorithms to differentiate between genuine and synthetic voice patterns. Additionally, the submission proposes a framework for increased public and private sector responsibility.

David Przygoda, the CEO of OmniSpeech said of issues involved in the Challenge: "Innovation in this area is crucial because Al-enabled voice cloning technology presents both an opportunity and a threat." Dr. Carol Espy-Wilson, the founder and CTO of OmniSpeech, said: "This award reaffirms our dedication to developing cutting-edge technology that not only advances Al voice capabilities but also prioritizes the safety and security of consumers against the latest Al voice clones."

"**DeFake**: Using Adversarial Audio Perturbations to Proactively Prevent Malicious Voice Cloning" (Video / Abstract). Submitted by Dr. Ning Zhang, an Assistant Professor in the Department of Computer Science and Engineering at Washington University in St. Louis. DeFake proposes a protective mechanism to add carefully crafted perturbations to voice samples to hinder the cyber criminal's cloning process.

According to Dr. Zhang: "While our solution is recognized for its potential, it remains a first step towards making a difference for society at large. This award will serve as a reminder that we now have a greater obligation to the billions of Al users out there."

"**OriginStory**: Authenticating the human origin of voice at the time of recording" (Video / Abstract). Submitted by Dr. Visar Berisha, Drena Kusari, Dr. Daniel W. Bliss, and Dr. Julie M. Liss of the small organization OriginStory. OriginStory proposes using off-the-shelf sensors already integrated in many devices to simultaneously measure speech acoustics and the co-occurring biosignals in the throat and mouth as a person is speaking, thus authenticating the human origin of voice recordings at the point of creation and embedding this authentication as a watermark or signature in the stream.

Dr. Berisha said of the Challenge: "It's exciting that the FTC has taken a leadership role in this space and we are honored to win the Voice Cloning Challenge. Our selection serves as further validation for our central thesis: we need new technology to establish a chain of trust that a voice is authentically human from the moment it is recorded to when it is listened to."

"**Voice Cloning Detection**" (Video / Abstract). Submitted by Pindrop Security (a large organization), including Dr. Elie Khoury, Anthony Stankus, Ketuman Sardesai, and Amanda Braun. "Voice Cloning Detection" purposes liveness detection technology to detect voice clones and audio deepfakes in real time.

Dr. Elie Khoury, the Vice President of Research at Pindrop, said of the issues involved in the Challenge: "Voice cloning and GenAI driven advanced speech and language tools have given scammers a potent weapon. A significant leapfrog in innovation is needed in the area of liveness detection, conversation security, and ethical use of AI to counter these threats before fraudsters cause long-term damage."

IV. Conclusion

The four FTC Voice Cloning Challenge winning submissions demonstrate the potential for cutting edge technology to help mitigate risks of voice cloning in the marketplace. They promote approaches that tap American innovation to help protect the public. The results of the Challenge also highlight that there is no single solution to this problem.

The FTC has had great success in the past with its four challenges to the public to help tackle unlawful robocalls.[17] We hope that the winners of the Voice Cloning Challenge will have similar success in coming to market as some of the winners our prior challenges, which built successful and sustaining business that are still helping consumers today.

Overall, with the threats posed by AI in mind, the FTC has made it clear that it is prepared to use all of its tools to prevent harm and hold bad actors accountable, including through law enforcement and rulemaking, as well as through consumer and business education, and by spurring innovation, as exemplified by the Voice Cloning Challenge. The FTC will continue this work, and will consistently remind industry that there is no AI exception to consumer protection or antitrust laws. We stand ready to work with the FCC and other agencies—both state and federal—to advance this critical goal.

---

[17] *See* Comment of the Fed. Trade Comm'n, In the matter of: Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, at 4 & nn.15-17 (July 3, 2017).