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

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 affir ms 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in the Children 's Online Privacy Protection Act Rule on the indefinite retention of children 's data are not superseded by claims from businesses that data must be indefinitely retained to improve machine learning algorithms.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).

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

e03 T-.008( )]TJ 8.Ia 02 (ishe (a)-1Ia)

3 .   w Req7udg (0)-g (d) Pdwow$7 0 Td [0)-

that can impact life and safety is worthy of our trust. Ove r 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.

x   Britt Paris , assistant professo r 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 Inter net 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 /(a)4 (l)]T Tw [(A)b Td[A(T)c7O(2h(0SM T8 gt(bH)9r) (STbm(6646 (

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 Sub

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).