



**Before the
Federal Trade Commission
Washington DC, 20580
In the Matter of the Request for Comment on AI Voice Impersonation
Rule, (Released Feb. 15, 2024)**

Comments of the American Consumer Institute

The American Consumer Institute is a nonprofit 501(c)(3) education and research organization. Its mission is to identify, analyze and protect the interests of consumers in legislative and rulemaking proceedings across various industries, including technology. The American Consumer Institute hereby submits these comments in response to the above-captioned proceeding.

Promises and pitfalls accompany any major advances in technology, and artificial intelligence (AI) is no exception. There are many existing applications of AI which yield consumer benefits plus applications no one has thought of yet. Unfortunately, there are those that seek to use this technology for nefarious purposes, but broad regulation could eliminate both the harm and the benefits from AI.

The Federal Trade Commission's (FTC) proposed rule on AI voice impersonations comes after a wave of scammers misrepresented their identity (frequently claiming to be a government official or a loved one) to extort money from unsuspecting victims. The FTC estimates that these scams have cost victims as much as \$4.6 billion.¹ This is a clear example of AI technology being used for fraudulent

¹ "As Nationwide Fraud Losses Top \$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public," *Federal Trade Commission*, February 9, 2024, accessed March 5, 2024, <https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>.

purposes and the FTC is right to try and stop it. However, in the process of carrying out enforcement action against scammers, it is critical that the FTC not harm legitimate users of AI voice cloning technology.

The new rule seeks to hold developers liable for the misuse of their voice cloning software.² Liability based on this standard would likely apply to companies who know, are “deliberately ignorant,” or “act in reckless disregard” to whether their technology is being used to defraud individuals.³

The standard is aimed at preventing guilty parties from turning a blind eye to the problem. Unfortunately, this leaves the question of how a developer of a general-purpose technology like AI voice cloning is supposed to know that their product is being misused unresolved. This will require the FTC to clarify the “knows or has reason to know” standard for using a very general-purpose technology and constructing the rule in a way that does not harm legitimate users, particularly those with disabilities that AI voice cloning could help.

Without clarifying this point, it is difficult to know when the creator of an AI product should be liable. Incorporating language to clarify this point would help better target the enforcement of this rule against scammers while sparing honest developers.

While the issue of AI-generated voices has not been tackled by the court, use of technology for illegal purposes has been addressed. For example, in *Twitter v. Taamneh* it was found that Twitter was not liable for ISIS using its algorithms to promote their propaganda due to difficulty in proving that the company knew about the misuse.⁴ In

² “FTC Proposes New Protections to Combat AI Impersonation of Individuals,” *Federal Trade Commission*, February 15, 2024, accessed March 5, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals?utm_source=govdelivery.

³ “13 CFR § 142.6 - What does the phrase ‘know or have reason to know’ mean?” *Cornell Law School Legal Information Institute*, accessed March 5, 2024, <https://www.law.cornell.edu/cfr/text/13/142.6>.

⁴ Henderson, Peter “Who Is Liable When Generative AI Says Something Harmful?” *Stanford University Human-Centered Artificial Intelligence* October 11, 2023, accessed March 14, 2024, [Who Is Liable When Generative AI Says Something Harmful? \(stanford.edu\)](https://hcr.stanford.edu/who-is-liable-when-generative-ai-says-something-harmful/).

addition, companies generally are not held liable for extreme misuse of their products.⁵ With this precedent, existing law seems to favor putting liability on the person who used the product for an illegal purpose rather than the developer who did not intend it to be used in such a manner.

Among the legitimate uses of voice cloning technology, one of the most promising is the ability to reinstate the voices of those with speaking disabilities. Assistive voice technology such as Whispp can assist people with speech impediments, who have limited ability to communicate verbally.⁶ With critical uses such as this in mind, it is important to design this rule around promising new technologies that assist people with their disabilities.

Combating fraud is a key aspect of the FTC's mission and sometimes updates to rules are necessary to keep up with emerging threats. However, it is important to do this while protecting honest developers and users. By focusing on the responsibility of the user, we can go after those who defraud individuals using voice cloning technology without unfairly penalizing developers who never intended for their software to be misused.

⁵ Copenhaver, Steven M “When Do Manufacturers Need to Anticipate Misuses – and Abuses – of Their Products?” *National Law Review* April 18, 2018, accessed March 14, 2024, [Product Use and Misuse \(natlawreview.com\)](https://natlawreview.com).

⁶ “Technology,” *Whispp*, accessed March 5, 2024, <https://whispp.com/technology/>.