Before the FEDERAL COMMUNICATIONS COMMISSION Washington, DC 20554

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

COMMENTS OF CONSUMER REPORTS



Grace Gedye Justin Brookman Consumer Reports 607 14th St NW, Suite 725 Washington, DC 20004 Consumer Reports writes in support of the Federal Communications Commission's (FCC) proposed rule regarding artificial intelligence-generated robocalls. We are pleased the Commission is taking action on this important issue. Unwanted calls are a persistent source of frustration for consumers, and the rise of AI technology may supercharge deception and fraud.

AI voice and audio tools offer a much higher level of conversational fluency than previous automated or pre-recorded messages, unlocking the possibility of much more lifelike – and potentially deceptive – robocalls. OpenAI offers a voice assistant product that can speak in fluid, realistic sentences, and quickly parse input speech. Google offers a similar product with Gemini Live. Already, consumers have been on the receiving end of calls that seemingly use AI voice tools to defraud or mislead them.

We support the Commission's proposal to require callers initiating AI-generated calls to disclose to the called party that the caller is using AI technology. With that information, consumers can end the call if they do not wish to proceed. If they decide to proceed, they'd be armed with the knowledge that they are not interacting with a human, and therefore would be less likely to experience confusion. If the disclosure is short and to the point, this is information that consumers can understand and act on.

We appreciate that the Commission seeks comment on the privacy implications of call detection, alerting, and blocking technologies. The content of consumers' phone calls is highly sensitive and highly private data. It reveals the nature of our most intimate relationships, health issues, proclivities and vulnerabilities. Call detection and blocking technologies can be useful to consumers, and there are steps companies can take to make their products more secure, such as running software locally on consumers' phones and not engaging in secondary data usage.

But while companies developing these technologies may initially offer products that respect consumers' privacy, there is little to stop them from later deciding that the content of consumers' calls is in fact valuable for other purposes—such as profiling and ad targeting. For example, after

¹ "ChatGPT Can Now See, Hear, and Speak." *Openai.com*, 2023, openai.com/index/chatgpt-can-now-see-hear-and-speak/.

² Davis, Wes. "Google Gemini's Voice Chat Mode Is Here." *The Verge*, 13 Aug. 2024, www.theverge.com/2024/8/13/24219553/google-gemini-live-voice-chat-mode. Accessed 4 Oct. 2024.

³ Harwell, Drew. "An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft." *Washington Post*, 4 Sept. 2019,

 $[\]underline{www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reported}\\ \underline{lv-used-major-theft/}.$

Verma, Pranshu. "They Thought Loved Ones Were Calling for Help. It Was an AI Scam." *Washington Post*, 5 Mar. 2023, www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/.

Schwartzman, Paul, and Pranshu Verma. "Baltimore Principal's Racist Rant Was an AI Fake. His Colleague Was Arrested." *Washington Post*, 26 Apr. 2024,

www.washingtonpost.com/dc-md-va/2024/04/26/baltimore-ai-voice-audio-framing-principal/.

Google acquired DoubleClick, an online advertising company, it initially kept the DoubleClick's massive stores of consumer browsing data separate from the names, email addresses, and other identifying information it gleaned from users thanks to Gmail logins and other Google products.⁴ Then, with a quiet change to its privacy policy in 2016, Google gave itself permission to merge that data and match named users to online ad tracking.⁵ Similarly, Meta used to promise that it wouldn't use the consumer data it gathered via 'Like' buttons embedded on sites across the internet for commercial purposes. 6 Then, in 2014, Meta changed its mind and announced that it would use the data it collected via the 'Like' button and other tools to track people online for ad targeting. Companies may say that they won't repurpose consumers' hypersensitive call data, but they don't have a good track record of sticking to their promises.

Consumer Reports supports the Commission's rulemaking, as do our members. Below we've attached a petition signed by more than 50,000 consumers in support of the rulemaking.

Respectfully submitted,

Grace Gedye Policy Analyst **Consumer Reports** 607 14th St NW, Suite 725 Washington, DC 20004

⁷ ibid

⁴ Angwin, Julia. "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking." *ProPublica*, 21 Oct. 2016, www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. ⁵ ibid

⁶ Angwin, Julia. "It's Complicated: Facebook's History of Tracking You." *ProPublica*, 17 June 2014, www.propublica.org/article/its-complicated-facebooks-history-of-tracking-vou.