TechXplore

Biden robocall: Audio deepfake fuels election disinformation fears

February 5 2024, by Anuj CHOPRA

Researchers are concerned about election disinformation fueled by AI deepfake audio.

The 2024 White House race faces the prospect of a firehose of AI-enabled disinformation, with a robocall impersonating US President Joe

Biden already stoking particular alarm about audio deepfakes.

"What a bunch of malarkey," said the phone message, digitally spoofing Biden's voice and echoing one of his signature phrases.

The robocall urged New Hampshire residents not to cast ballots in the Democratic primary last month, prompting state authorities to launch a probe into possible voter suppression.

It also triggered demands from campaigners for stricter guardrails around generative artificial intelligence tools or an outright ban on robocalls.

Disinformation researchers fear rampant misuse of AI-powered applications in a pivotal election year thanks to proliferating voice cloning tools, which are cheap and easy to use and hard to trace.

"This is certainly the tip of the iceberg," Vijay Balasubramaniyan, chief executive and co-founder of cybersecurity firm Pindrop, told AFP.

"We can expect to see many more deepfakes throughout this election cycle."

A detailed analysis published by Pindrop said a text-to-speech system developed by the AI voice cloning startup ElevenLabs was used to create the Biden robocall.

The scandal comes as campaigners on both sides of the US political aisle harness advanced AI tools for effective campaign messaging and as tech investors pump millions of dollars into voice cloning startups.

Balasubramaniyan refused to say whether Pindrop had shared its findings with ElevenLabs, which last month announced a financing round from investors that, according to Bloomberg News, gave the firm a valuation of $1.1 billion.

ElevenLabs did not respond to repeated AFP requests for comment. Its website leads users to a free text-to-speech generator to "create natural AI voices instantly in any language."

Under its safety guidelines, the firm said users were allowed to generate voice clones of political figures such as Donald Trump without their permission if they "express humor or mockery" in a way that makes it "clear to the listener that what they are hearing is a parody, and not authentic content."

'Electoral chaos'

US regulators have been considering making AI-generated robocalls illegal, with the fake Biden call giving the effort new impetus.

"The political deepfake moment is here," said Robert Weissman, president of the advocacy group Public Citizen.

"Policymakers must rush to put in place protections or we're facing electoral chaos. The New Hampshire deepfake is a reminder of the many ways that deepfakes can sow confusion."

Researchers fret the impact of AI tools that create videos and text so seemingly real that voters could struggle to decipher truth from fiction, undermining trust in the electoral process.

But audio deepfakes used to impersonate or smear celebrities and politicians around the world have sparked the most concern.

"Of all the surfaces—video, image, audio—that AI can be used for voter suppression, audio is the biggest vulnerability," Tim Harper, a senior policy analyst at the Center for Democracy & Technology, told AFP.

"It is easy to clone a voice using AI, and it is difficult to identify."

'Election integrity'

The ease of creating and disseminating fake audio content complicates an already hyperpolarized political landscape, undermining confidence in the media and enabling anyone to claim that fact-based "evidence has been fabricated," Wasim Khaled, chief executive of Blackbird.AI, told AFP.

Such concerns are rife as the proliferation of AI audio tools outpaces detection software.

China's ByteDance, owner of the wildly popular platform TikTok, recently unveiled StreamVoice, an AI tool for real-time conversion of a user's voice to any desired alternative.

"Even though the attackers used ElevenLabs this time, it is likely to be a different generative AI system in future attacks," Balasubramaniyan said.

"It is imperative that there are enough safeguards available in these tools."

Balasubramaniyan and other researchers recommended building audio watermarks or digital signatures into tools as possible protections as well as regulation that makes them available only for verified users.

"Even with those actions, detecting when these tools are used to generate harmful content that violates your terms of service is really hard and really expensive," Harper said.

"(It) requires investment in trust and safety and a commitment to building with election integrity centred as a risk."

Citation: Biden robocall: Audio deepfake fuels election disinformation fears (2024, February 5) retrieved 1 May 2024 from https://techxplore.com/news/2024-02-biden-robocall-audio-deepfake-fuels.html