THE HILL: TECHNOLOGY

Fake Biden robocall 'tip of the iceberg' for AI election misinformation

BY REBECCA KLAR - 01/24/24 6:00 AM ET

A digitally altered message created to sound like President Biden urging New Hampshire residents not to vote in Tuesday's primary added fuel to calls for regulation of artificial intelligence (AI) as the 2024 campaign heats up.

The robocall is the latest example of how AI is being used in elections as the U.S. lacks fundamental guardrails to curtail threats posed by the technology, which can make it appear a candidate is saying or doing something that never happened.

As the technology becomes harder to detect and easier for anyone to use, experts said more AI election content will likely emerge, which could sow confusion and distrust among voters.

"This is kind of just the tip of the iceberg in what could be done with respect to voter suppression or attacks on election workers," said Kathleen Carley, a professor at Carnegie Mellon University.

"It was almost a harbinger of what all kinds of things we should be expecting over the next few months," she added.

Samir Jain, vice president of policy at the Center for Democracy and Technology (CDT), said the robocall highlighted two risks posed by deceptive AI election content: It made a candidate appear to say something they did not, and it spread false information about voting.

A spokesperson for the campaign to write in Biden's name on the New Hampshire primary ballot slammed the robocall, which was first reported by NBC News, as a form of "deepfake disinformation designed to harm Joe Biden, suppress votes, and damage our democracy."

The robocall campaign is under investigation by New Hampshire regulators and triggered a call from New York Democratic Rep. Joseph Morelle for an investigation by the Justice Department.

In addition to the risks of replicating a candidate's likeness, AI advances also make it easier to target specific groups with misinformation campaigns. The large language models that power AI systems could be used to generate a model of a potential audience, Carley said.

Just like an AI system could produce a song in the style of a certain genre or artist, Carley said, AI "could take the same misleading story" and "tell it in different ways" that are tailored to the style a particular audience would like.

The advances also raise concerns about attacks on election workers and trust in the process. For example, AI could be used to generate videos that falsely appear to show election workers tampering with votes, Carley said.

"It's 100 percent certainty in the absence of laws making deepfakes illegal or requiring disclosure that political operatives of all stripes and all levels of government will use the technology to advance their interests, irrespective of the impact on the broader democracy," said Robert Weissman, president of the nonprofit watchdog group Public Citizen.

The advocacy group led a petition urging the Federal Election Commission (FEC) to amend its rules about fraudulently misrepresenting candidates or political parties to make it clear that it applies to deliberately deceptive AI in campaigns.

The FEC unanimously voted in August to open a public comment period about updating the rule. The commission has yet to make an update since closing the public comment period in October.

Public Citizen has slammed the FEC for moving slowly on the matter.

A spokesperson for the FEC said Tuesday they do not have an update on timing to share. The spokesperson also directed The Hill to a statement from FEC Chair Sean J. Cooksey (R) to The Washington Post that pushed back on criticism of moving slowly.

"Any suggestion that the FEC is not working on the pending AI rulemaking petition is false. The Commission and its staff are diligently reviewing the thousands of public comments submitted. When that process is complete, I expect the Commission will resolve the AI rulemaking by early summer," Cooksey said.

Weissman said the New Hampshire robocall underscores the need for swift action.

"The political deepfake era is here and regulators are either going to step up or we're going to descend into election chaos," he said.

Weissman said the FEC's action is crucial not just because of what rule it can issue, but also to establish the "social and legal norm that political deepfakes are not okay."

At the same time, he said the FEC's authority is limited to the reach of candidates and political parties meaning it wouldn't address content by outside political spenders or just individuals posting on social media. To target those concerns, he said there needs to be a more comprehensive Congressional action.

Although there is bipartisan interest, Weissman said it is "unwise to bet on Congress to do anything on any topic at this point."

Sen. Amy Klobuchar (D-Minn.) pushed her bipartisan bill, co-sponsored by Sens. Josh Hawley (R-Mo.), Chris Coons (D-Del.) and Susan Collins (R-Maine), that seeks to prohibit the distribution of materially deceptive AI-generated audio, images or video in political ads as a way to mitigate risks such as the New Hampshire robocall.

"These AI-created deepfakes of candidates are dangerous to our democracy, and we're already starting to see this happen with the reported fake robocall using the President's voice to tell people not to vote in New Hampshire. Whether you are a Democrat or a Republican, no one wants to see fake ads or robocalls where you cannot even tell if it's your candidate or not," Klobuchar said in a statement Monday.

In lieu of federal guidelines, states are also pushing ahead with action. California, Michigan, Minnesota, Texas and Washington have enacted laws to regulate deepfakes in elections, and about two dozen more have introduced or discussed such regulations, according to a tracker compiled by Public Citizen.

Jain said the risks posed by AI election content is an "ecosystem-wide problem" that will require action by government, political campaigns, and private companies to help mitigate the threats.

Major social media and AI companies have rolled out policies that require the disclosure of generative AI in political ads. OpenAI, the company behind the popular ChatGPT tool, also released a plan to prevent the use of its tools to spread election misinformation, including banning people from using its tech to create chatbots that impersonate real candidates.

Already, OpenAI implemented the policy to ban a bot imitating Democratic presidential candidate Rep. Dean Phillips (Minn.).

Jain said it's crucial that private companies don't just have policies in place, but also back them up with resources and enforcement.

"Without those two steps, it really doesn't matter what the policies are," he said.