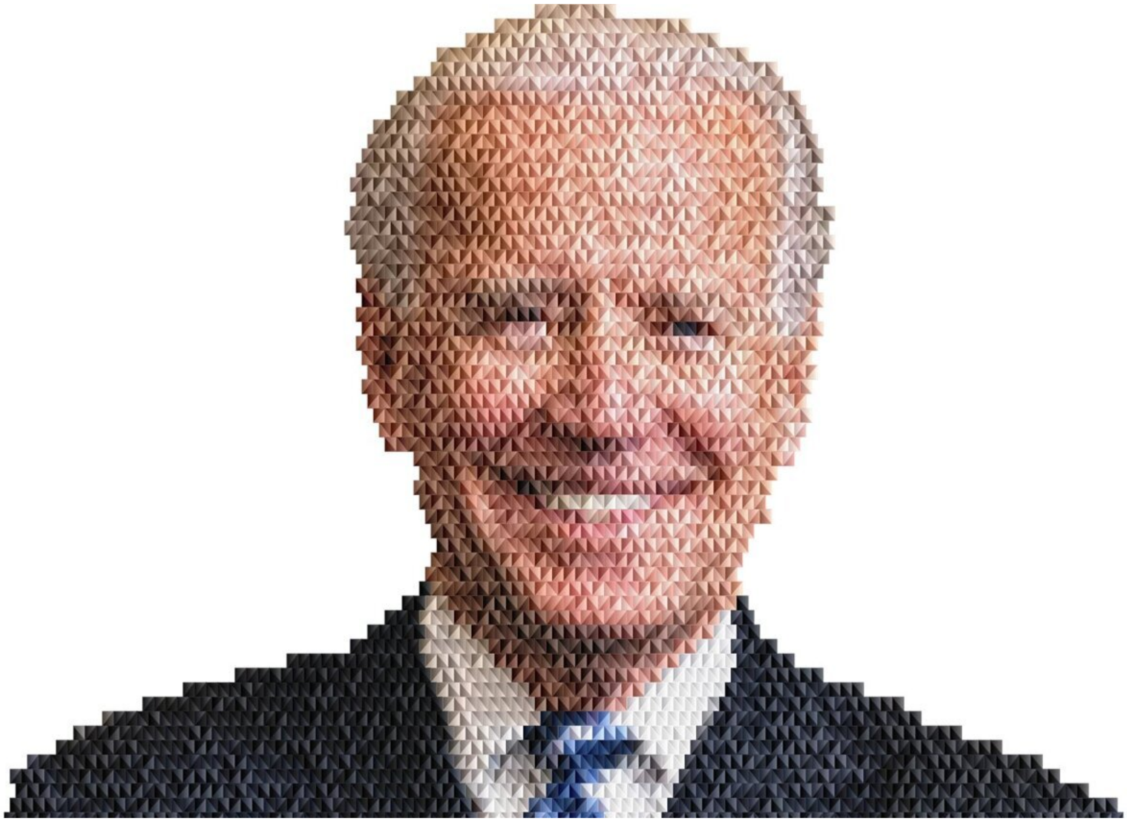
Fake Biden robocall to New Hampshire voters highlights how easy it is to make deepfakes

January 24 2024, by Joan Donovan



Credit: Pixabay/CC0 Public Domain

An unknown number of New Hampshire voters received a phone call on Jan. 21, 2024, from what sounded like President Joe Biden. A recording contains Biden's voice urging voters inclined to support Biden and the Democratic Party not to participate in New Hampshire's Jan. 23 GOP primary election.

"Republicans have been trying to push nonpartisan and Democratic voters to participate in their primary. What a bunch of malarkey. We know the value of voting Democratic when our votes count. It's important that you save your vote for the November election. We'll need your help in electing Democrats up and down the ticket. Voting this Tuesday only enables the Republicans in their quest to elect Donald Trump again. Your vote makes a difference in November, not this Tuesday. If you would like to be removed from future calls, please press two now."

The call falsely implies that a registered Democrat could vote in the Republican primary and that a voter who votes in the primary would be ineligible to vote in the general election in November. The state does allow unregistered voters to participate in either the Republican or Democratic primary.

The call, two days before the primary, appears to have been an artificial intelligence deepfake. It also appears to have been an attempt to discourage voting. Biden is not on the ballot because of a dispute between the Democratic National Committee and New Hampshire Democrats about New Hampshire's position in the primary schedule, but there is a write-in campaign for Biden.

Robocalls in elections are nothing new and not illegal; many are simply efforts to get out the vote. But they have also been used in voter suppression campaigns. Compounding this problem in this case is what I believe to be the application of AI to clone Biden's voice.

In a media ecosystem full of noise, scrambled signals such as deepfake robocalls make it virtually impossible to tell facts from fakes.

Recently, a number of companies have popped up online offering impersonation as a service. For users like you and me, it's as easy as selecting a politician, celebrity or executive like Joe Biden, Donald Trump or Elon Musk from a menu and typing a script of what you want them to appear to say, and the website creates the deepfake automatically. Though the audio and video output is usually choppy and stilted, when the audio is delivered via a robocall it's very believable. You could easily think you are hearing a recording of Joe Biden, but really it's machine-made misinformation.

Context is key

I'm a media and disinformation scholar. In 2019, information scientist Brit Paris and I studied how generative adversarial networks—what most people today think of as AI—would transform the ways institutions assess evidence and make decisions when judging realistic-looking audio and video manipulation. What we found was that no single piece of media is reliable on its face; rather, context matters for making an interpretation.

When it comes to AI-enhanced disinformation, the believability of deepfakes hinges on where you see or hear it or who shares it. Without a valid and confirmed source vouching for it as a fact, a deepfake might be interesting or funny but will never pass muster in a courtroom. However, deepfakes can still be damaging when used in efforts to suppress the vote or shape public opinion on divisive issues.

AI-enhanced disinformation campaigns are difficult to counter because unmasking the source requires tracking the trail of metadata, which is the data about a piece of media. How this is done varies, depending on the method of distribution: robocalls, social media, email, text message or websites. Right now, research on audio and video manipulation is more difficult because many big tech companies have shut down access to their application programming interfaces, which make it possible for researchers to collect data about social media, and the companies have laid off their trust and safety teams.

Timely, accurate, local knowledge

In many ways, AI-enhanced disinformation such as the New Hampshire robocall poses the same problems as every other form of disinformation. People who use AI to disrupt elections are likely to do what they can to hide their tracks, which is why it's necessary for the public to remain skeptical about claims that do not come from verified sources, such as local TV news or social media accounts of reputable news organizations.

It's also important for the public to understand what new audio and visual manipulation technology is capable of. Now that the technology has become widely available, and with a pivotal election year ahead, the fake Biden robocall is only the latest of what is likely to be a series of AI-enhanced disinformation campaigns.

I believe society needs to learn to venerate what I call TALK: timely, accurate, local knowledge. I believe that it's important to design social media systems that value timely, accurate, local knowledge over disruption and divisiveness.

It's also important to make it more difficult for disinformers to profit from undermining democracy. For example, the malicious use of technology to suppress voter turnout should be vigorously investigated by federal and state law enforcement authorities.

While deepfakes may catch people by surprise, they should not catch us off guard, no matter how slow the truth is compared with the speed of disinformation.

Provided by The Conversation

Citation: Fake Biden robocall to New Hampshire voters highlights how easy it is to make deepfakes (2024, January 24) retrieved 11 May 2024 from https://techxplore.com/news/2024-01-fake-biden-robocall-hampshire-voters.html