# I never said that! High-tech deception of 'deepfake' videos

July 2 2018, by Deb Riechmann

This image made from video of a fake video featuring former President Barack Obama shows elements of facial mapping used in new technology that lets anyone make videos of real people appearing to say things they've never said. There is rising concern that U.S. adversaries will use new technology to make authentic-looking videos to influence political campaigns or jeopardize national security. (AP Photo)

Hey, did my congressman really say that? Is that really President Donald Trump on that video, or am I being duped?

New technology on the internet lets anyone make videos of real people appearing to say things they've never said. Republicans and Democrats predict this high-tech way of putting words in someone's mouth will become the latest weapon in disinformation wars against the United States and other Western democracies.

We're not talking about lip-syncing videos. This technology uses facial mapping and artificial intelligence to produce videos that appear so genuine it's hard to spot the phonies. Lawmakers and intelligence officials worry that the bogus videos—called deepfakes—could be used to threaten national security or interfere in elections.

So far, that hasn't happened, but experts say it's not a question of if, but when.

"I expect that here in the United States we will start to see this content in the upcoming midterms and national election two years from now," said Hany Farid, a digital forensics expert at Dartmouth College in Hanover, New Hampshire. "The technology, of course, knows no borders, so I expect the impact to ripple around the globe."

When an average person can create a realistic fake video of the president saying anything they want, Farid said, "we have entered a new world where it is going to be difficult to know how to believe what we see." The reverse is a concern, too. People may dismiss as fake genuine footage, say of a real atrocity, to score political points.

Realizing the implications of the technology, the U.S. Defense Advanced Research Projects Agency is already two years into a four-year program to develop technologies that can detect fake images and videos. Right now, it takes extensive analysis to identify phony videos. It's unclear if new ways to authenticate images or detect fakes will keep pace with deepfake technology.

Deepfakes are so named because they utilize deep learning, a form of artificial intelligence. They are made by feeding a computer an algorithm, or set of instructions, lots of images and audio of a certain person. The computer program learns how to mimic the person's facial expressions, mannerisms, voice and inflections. If you have enough video and audio of someone, you can combine a fake video of the person with a fake audio and get them to say anything you want.

So far, deepfakes have mostly been used to smear celebrities or as gags, but it's easy to foresee a nation state using them for nefarious activities against the U.S., said Sen. Marco Rubio, R-Fla., one of several members of the Senate intelligence committee who are expressing concern about deepfakes.

A foreign intelligence agency could use the technology to produce a fake video of an American politician using a racial epithet or taking a bribe, Rubio says. They could use a fake video of a U.S. soldier massacring civilians overseas, or one of a U.S. official supposedly admitting a secret plan to carry out a conspiracy. Imagine a fake video of a U.S. leader—or an official from North Korea or Iran—warning the United States of an impending disaster.

"It's a weapon that could be used—timed appropriately and placed appropriately—in the same way fake news is used, except in a video form, which could create real chaos and instability on the eve of an election or a major decision of any sort," Rubio told The Associated Press.

Deepfake technology still has a few hitches. For instance, people's blinking in fake videos may appear unnatural. But the technology is improving.

"Within a year or two, it's going to be really hard for a person to

distinguish between a real video and a fake video," said Andrew Grotto, an international security fellow at the Center for International Security and Cooperation at Stanford University in California.

"This technology, I think, will be irresistible for nation states to use in disinformation campaigns to manipulate public opinion, deceive populations and undermine confidence in our institutions," Grotto said. He called for government leaders and politicians to clearly say it has no place in civilized political debate.

Crude videos have been used for malicious political purposes for years, so there's no reason to believe the higher-tech ones, which are more realistic, won't become tools in future disinformation campaigns.

Rubio noted that in 2009, the U.S. Embassy in Moscow complained to the Russian Foreign Ministry about a fake sex video it said was made to damage the reputation of a U.S. diplomat. The video showed the married diplomat, who was a liaison to Russian religious and human rights groups, making telephone calls on a dark street. The video then showed the diplomat in his hotel room, scenes that apparently were shot with a hidden camera. Later, the video appeared to show a man and a woman having sex in the same room with the lights off, although it was not at all clear that the man was the diplomat.

John Beyrle, who was the U.S. ambassador in Moscow at the time, blamed the Russian government for the video, which he said was clearly fabricated.

Michael McFaul, who was American ambassador in Russia between 2012 and 2014, said Russia has engaged in disinformation videos against various political actors for years and that he too had been a target. He has said that Russian state propaganda inserted his face into photographs and "spliced my speeches to make me say things I never uttered and even

accused me of pedophilia."