CHAIRMAN ADAM B. SCHIFF

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

NATIONAL SECURITY CHALLENGES OF ARTIFICIAL INTELLIGENCE, MANIPULATED MEDIA, AND "DEEPFAKES"

JUNE 13, 2019

In the heat of the 2016 election as the Russian hacking and dumping operation became apparent, my predominant concern was that the Russians would begin dumping forged documents along with the ones they stole. It would be all too easy for Russia, or another malicious actor to seed forged documents among the authentic ones in a way that would make them almost impossible to identify or rebut. Even if a victim could ultimately expose the forgeries for what they were, the damage would be done.

Three years later we are on the cusp of a technological revolution that could enable even more sinister forms of deception and disinformation by malign actors, foreign or domestic. Advances in AI and machine learning have led to the emergence of advanced digitally doctored types of media, so-called "deepfakes,"that enable malicious actors to foment chaos, division or crisis and they have the capacity to disrupt entire campaigns, including that for the presidency.

Rapid progress in artificial intelligence algorithms has made it possible to manipulate media – video, imagery, audio, and text – with incredible, nearly imperceptible results. With sufficient training data, these powerful deepfake-generating algorithms can portray a real person doing something they never did, or saying words they never uttered.

These tools are readily available and accessible to both experts and novices alike, meaning that attribution of a deepfake to a specific author – whether a hostile intelligence service or a single Internet troll – will be a constant challenge.

What's more, once someone views a fake video, the damage is done. Even if later convinced that what they have seen is a forgery, that person may never lose completely the lingering negative impression the video has left them. It is also the case, that not only may fake videos be passed off as real, but real information can be passed off as fake. This is called the liars dividend, in which people with a propensity to deceive are given the benefit of an environment in which it is increasingly difficult for the public to determine what is true.

To give our Members and the audience a sense of the quality of deepfakes today, I want to show a few short examples.

1. The first comes from Bloomberg Businessweek, demonstrating an AI-powered cloned voice of one of its journalists.

2. The second clip, comes from Quartz and demonstrates a “puppet master” type of deepfake video. As you can see, these people are able to co-opt the head movements of their targets. If married with convincing audio, you can turn a world leader into a ventriloquist dummy.

3. Next, a brief CNN clip highlighting new
research from Professor Hany Farid, an acclaimed expert on deepfakes from UC Berkeley, and featuring an example of a so-called “face swap” video in which Senator Elizabeth Warren’s face is seamlessly transplanted on the body of SNL cast member Kate McKinnon

4. These algorithms can also learn from pictures of real faces to make completely artificial portraits of persons who do not exist at all. Can anyone here pick out which of these faces are real, and which are fake? As you may have guessed, all four were synthetically built with the assistance of AI.

Thinking ahead to 2020 and beyond, one does not need any great imagination to envision even more nightmarish scenarios that would leave the government, the media, and the public struggling to discern what is real and what is fake:

- A state-backed actor creates a deepfake video of a political candidate accepting a bribe, with the goal of influencing an election;

- An individual hacker claims to have stolen audio of a private conversation between two world leaders, when in fact no such conversation took place;

- A troll farm uses text-generating algorithms to write false or sensational news stories at scale, flooding social media platforms and overwhelming journalists' ability to verify, and users' ability to trust what they are reading.

What enables deepfakes and other modes of disinformation to become truly pernicious is the ubiquity of social media, and the velocity at which false information can spread. We got a preview of what that might look like recently when a doctored video of Speaker Nancy Pelosi went viral on Facebook, receiving millions of views in the span of 48 hours.

This video was not an AI assisted deepfake, but rather a crude, manual manipulation that some have termed a “cheap fake.” Nonetheless, the video’s virality on social media demonstrates the scale of the challenge we face, and the responsibilities that social media companies must confront. Already, the companies have taken different approaches, with YouTube deleting the altered video of Speaker Pelosi, while Facebook labeled it as false and throttled back its spread once it was deemed fake by independent factcheckers.

Now is the time for social media companies to put in place policies to protect users from misinformation, not in 2021 after viral deepfakes have polluted the 2020 elections. By then, it will be too late.

And so, in keeping with the series of open hearings that have examined different strategic challenges to our national security and our democratic institutions, the Committee is devoting this hearing to the deepfakes and synthetic media.

We need to soberly understand the implications of deepfakes, the underlying AI technologies, and the Internet platforms that give them reach, before we consider appropriate steps to mitigate the potential harms.

We have a distinguished panel of experts and practitioners to help us understand and contextualize the potential threat of deepfakes, but before turning to them, I would like to recognize Ranking Member Nunes for any opening statement he wishes to give.