Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY   (202) 225–5074
MINORITY   (202) 225–5051

https://oversight.house.gov

Ranking Member Gerald E. Connolly
Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Hearing on Hearing on "Advances in Deepfake Technology"
November 8, 2023

When most people hear the term "deepfake," this image may jump to mind. While images like this might make deepfakes seem innocuous, most of them are quite insidious. Take this AI-generated image for example.

Since the armed conflict between Israel and Hamas first broke out, false images, created by generative technology, have proliferated throughout the internet. As a result, these synthetic images have created a "algorithmically-driven fog of war," making it significantly more difficult to differentiate between truth and fiction.

And just last year, at the outset of Russia's invasion in Ukraine, a fabricated video of Ukrainian President Zelenskyy calling for Ukrainian soldiers to lay down their weapons circulated on social media. The video was a deepfake, but thanks to Ukraine's quick response to Russian disinformation, it was quickly debunked. Welcome to the new frontier of disinformation.

Geopolitics are one realm of deepfakes, but let's look at some numbers. According to one study, 96% of deepfake videos are of non-consensual pornography—96%! Another report confirmed that deepfake pornography almost exclusively targets and harms women. Knowing this, it should be no surprise that the very first deepfake ever created depicted the face of a famous female celerity superimposed onto the body of an actor in a pornographic video. And these kinds of manipulated videos are already affecting students in our schools back home. In one instance, a group of high school students in New Jersey used the images of a dozen female classmates to make AI pornography of their likenesses and spread it across campus. This is wrong and we need to stop it now.

Earlier this year, House Administration Committee Ranking Member Joe Morelle introduced a bill called the "The Preventing Deepfakes of Intimate Images Act." This bill bans the non-consensual sharing of synthetic intimate images and creates additional legal courses of action for those impacted. I am a cosponsor of this legislation and urge my colleagues to join me in support of this important bill. Congress must not shy away from preventing the harmful proliferation of deepfake pornography.

But it's not just deepfake videos that we have to worry about. With AI, scammers have the ability to easily create audio that mimics a person's voice, matching their age, gender, and tone. Thousands of Americans are scammed over the telephone every year using this technology, and deepfake capabilities further exacerbate the problem.

So, what can we do? AI image detecting tools are being developed and used to help verify the authenticity of machine generated images. Other tools place watermarks on AI-generated media to indicate that the media is synthetically created.

While these tools improve and evolve, both the public and the private sector must cooperate to educate the public on where these tools are and how to use them. **Government and the private sector must collaboratively highlight the dangers and consequences of deepfakes and teach how to combat this misinformation and prevent its abuses.**

Private developers must implement policies that preserve the integrity of truth and provide transparency to users. That is why I joined a letter, led by Rep. Kilmer and the New Dem Coalition's AI Working Group, that requests leaders of prominent generative AI and social media platforms provide information to Congress outlining their efforts to monitor, identify, and disclose deceptive synthetic media content.

And the public sector is already taking bold, consequential steps toward collaborative and comprehensive solutions. I applaud the efforts of the Biden-Harris Administration to secure commitments from seven major artificial intelligence companies to help users identify when content is AI generated and when it's not.

The Biden-Harris Administration took a resolute and unprecedented step last week when it issued its executive order on artificial intelligence. The sweeping executive order speaks directly to the issues we seek to examine today. It leans on tools like watermarking that can help people identify whether what they're looking at online is an authentic government document or a tool of misinformation.

The order instructs the Secretary of Commerce to work enterprise-wide to develop standards and best practices for detecting fake content and tracking the provenance of authentic information—and seeks to build partnerships and foster trust among the public and private sectors.

I trust this Subcommittee will conduct meaningful oversight of these efforts because we, as a nation, need to get this right. And I'm proud that the Biden-Harris Administration for taking the first step and performing its role as the global leader in addressing generative technology. I also look forward to hearing more today about existing and evolving private sector solutions. I want to learn more about the federal government's potential role in incentivizing solutions that keep pace with bad actors.

We already know Congress must continue to fund essential research programs that support the development of more advanced and effective deepfake detection tools. Funding for research through the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF) is critical to this important work. That requires a fully funded government. I once again call upon my colleagues across the aisle to fulfill their constitutional duty and work with Democrats to pass a bipartisan, long-term funding agreement.

I thank Chairwoman Mace for holding this hearing and emphasizing the harm of deepfakes and disinformation. I look forward to working with her on real solutions that get at the root of the truth decay problem.

Finally, Madam Chairwoman, I'd like to enter into the record a study published by Danielle Citron and Robert Chesney titled "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" that examines the harms of deepfakes and different policy proposals to protect the privacy and safety of Americans.

<div align="center">###</div>

Contact: Nelly Decker, Communications Director, (202) 226-5181