Statement for the Record

Dr. David Doermann

Professor, SUNY Empire Innovation

Interim Chair, Computer Science and Engineering

University at Buffalo, Buffalo, NY

FOR A HEARING ON

Recent advances in the creation and distribution of computer-generated images and voice cloning

BEFORE THE

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Committee on Oversight and Accountability

United States House of Representatives

Wednesday, November 8th, 2023

Chairwomen Mace, Ranking Member Connolly, and Honorable Members of Congress:

I appreciate the opportunity to testify before you today on the pressing issue of deepfake technology, creating and distributing computer-generated images and voice cloning. As these technologies advance at an unprecedented rate, it is crucial to recognize the potential for both positive and negative implications. Every week, we hear of its use at both ends of the spectrum. This week, we heard about AI being used to finish a new Beatles song on one hand and to generate nude images of classmates by a high schooler in New Jersey on the other. Despite our president's executive orders and testimony of thought leaders, we are not moving fast enough to curtail the continued damage this technology is doing and will continue to do as it evolves. Today, my testimony will provide an overview of recent advances, the misuse of deepfakes, and potential avenues for addressing these challenges.

In recent years, deepfake technology has made significant strides. Advances in machine learning, particularly the use of Generative Adversarial Networks (GANs), have created increasingly realistic and convincing deepfake content. These tools have also become more accessible and user-friendly, requiring less technical expertise, which is a double-edged sword as it can be used for creative and malicious purposes. The most immediate concern surrounding deepfakes is their misuse. They have been employed to spread fake news, disinformation campaigns, and political manipulation. Deepfake technology has sometimes been harnessed for extortion, blackmail, and identity theft. Additionally, it has been used in non-consensual pornography, cyberbullying, and harassment, causing severe harm to individuals. Furthermore, the potential national security implications are grave. Deepfakes can be exploited to impersonate government officials, military personnel, or law enforcement, leading to misinformation and potentially dangerous situations. The creation of misleading videos that could lead to diplomatic crises or escalate international tensions is a real threat.

The proliferation of deepfake technology is also eroding trust in digital media. It has become increasingly challenging for the public to distinguish between real and manipulated content. This erosion of trust affects media credibility and individuals' ability to make informed decisions based on the information they encounter. As we have seen countless times when trust is eroded, the public does not know what to believe, which opens the doors to the further proliferation of misinformation. One of my greatest concerns is when I hear people say that this is just the cost of progress. People, real people, are being hurt, and even if we have laws on the books that could be applied, our system is not ready to deal with these challenges and the speed at which technology is changing. We simply do not know what the future may hold, but if the trend continues, things will get much worse before they get better.

Detecting deepfakes is an ongoing challenge as the technology evolves to evade existing detection methods. However, ongoing research and industry efforts to develop more effective deepfake

detection tools need continued support. Before this technology had evolved, I started a program at DARPA called MediFor that focused on Media Forensics. As I am sure you know, DARPA focuses on preventing strategic surprise, but few imagined a decade ago the impact that this technology would have.

Let there be no question that this is a race. The better the generators and manipulators get, the better our solutions to combat them need to be. Unfortunately, when it comes to the harm, this is a race we will likely never win. Nevertheless, with a complete portfolio of technical, social, and legislative actions to damper the negative and advance the positive aspects of this technology. We must close the gap and continue to make it less attractive (financially, socially, politically) to propagate false information using these tools. We must be able to look to colleagues, to our role models, and to our leaders to set an example of what is acceptable and demand change.

I urge Congress to consider legislation and regulations to address the misuse of deepfake technology. Striking the right balance between free speech and safeguards to protect against malicious uses of deepfakes is essential. First and foremost, public awareness and digital literacy programs are vital in helping individuals recognize deepfakes and false information. We should consider including school media literacy education and promoting critical thinking skills. Collaboration between Congress and technology companies is essential to address the challenges posed by deepfakes. Tech companies are responsible for developing and implementing policies to detect and mitigate deepfake content on their platforms. More robust privacy and consent laws are needed to protect individuals from using their likeness and voice in deepfake content without their permission. Continued research and development in AI and deepfake technology are necessary, as is funding for initiatives to counter deepfake misuse.

In conclusion, deepfake technology offers innovative possibilities but severely threatens our society. We must act proactively to address these challenges and mitigate potential harm. I look forward to working with Congress and relevant stakeholders to find practical, balanced solutions that protect our digital landscape and uphold the values of transparency and trust.

Thank you for your attention, and I look forward to continuing this discussion.