Generative AI (Deepfakes)

Text-to-Image

“A realistic photo of the bombing at the Pentagon”

Text-to-Image

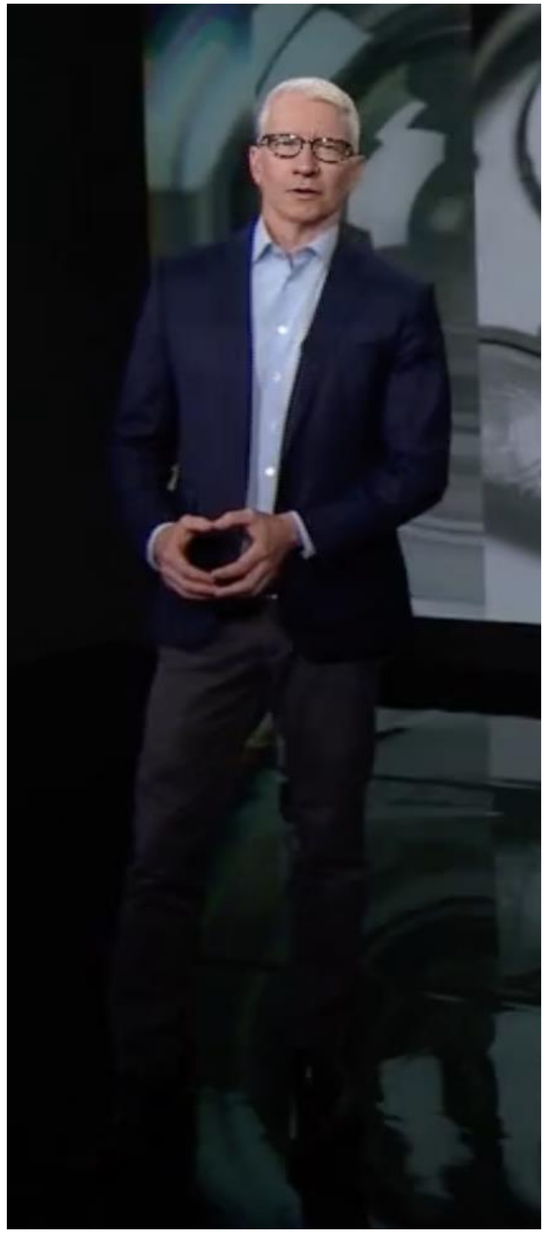
additive noise

denoise

“A diverse group of people sitting at the bar in an elegant wine tasting lounge in Northern California, drinking and chatting.”

Beautiful, snowy Tokyo city is bustling. The camera moves through the bustling city street, following several people enjoying the beautiful snowy weather and shopping at nearby stalls. Gorgeous sakura petals are flying through the wind along with snowflakes

Audio



Audio

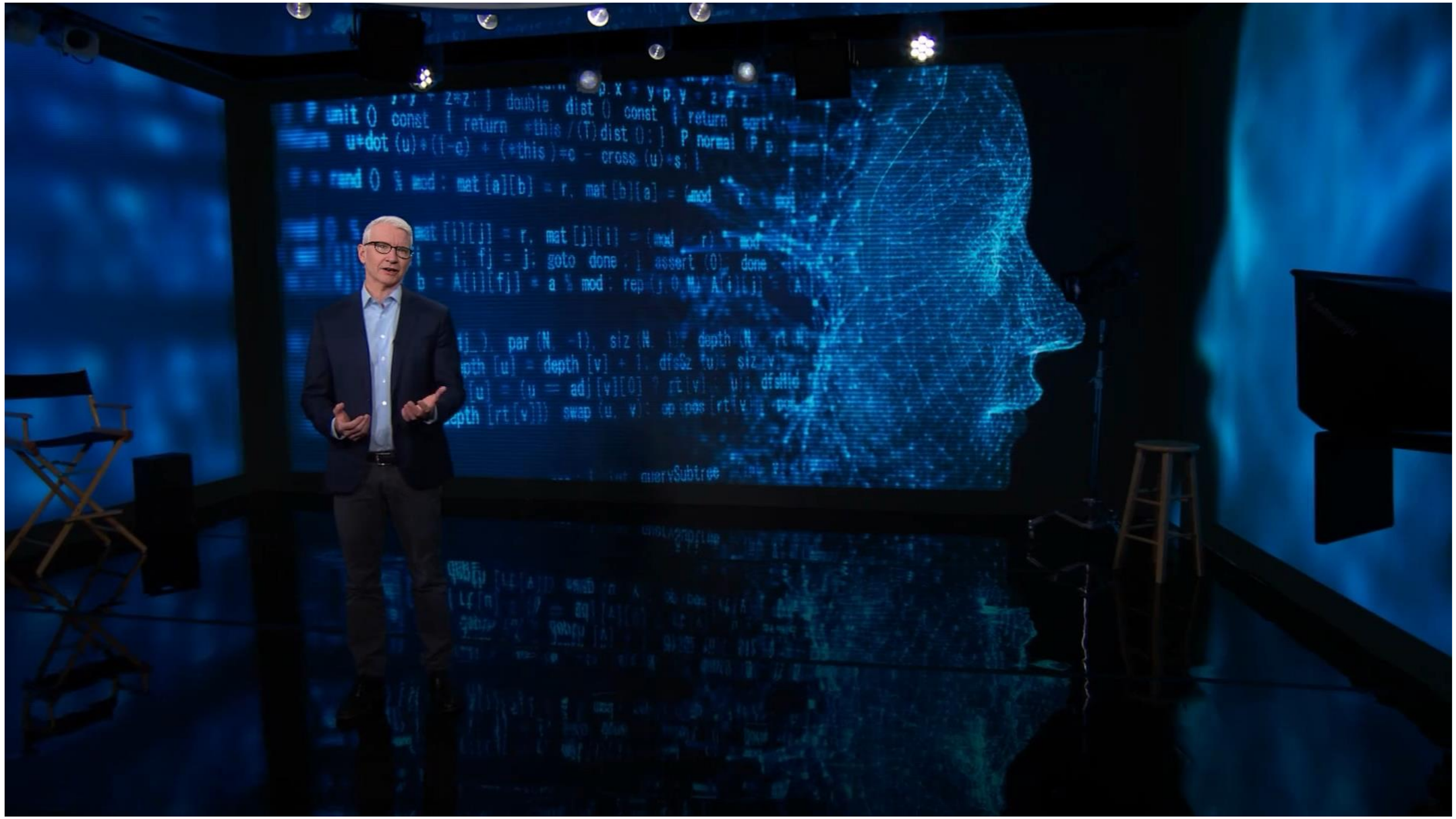
How a magician who has never voted found himself at the center of an AI political scandal

By Casey Tolan, Majlie de Puy Kamp and Kyung Lah, CNN

7 minute read · Published 6:14 PM EST, Fri February 23, 2024

Street magician Paul Carpenter said he used AI to create the fake audio of President Biden that was used in a robocall sent to New Hampshire voters. Courtesy Paul Carpenter

Video



Video

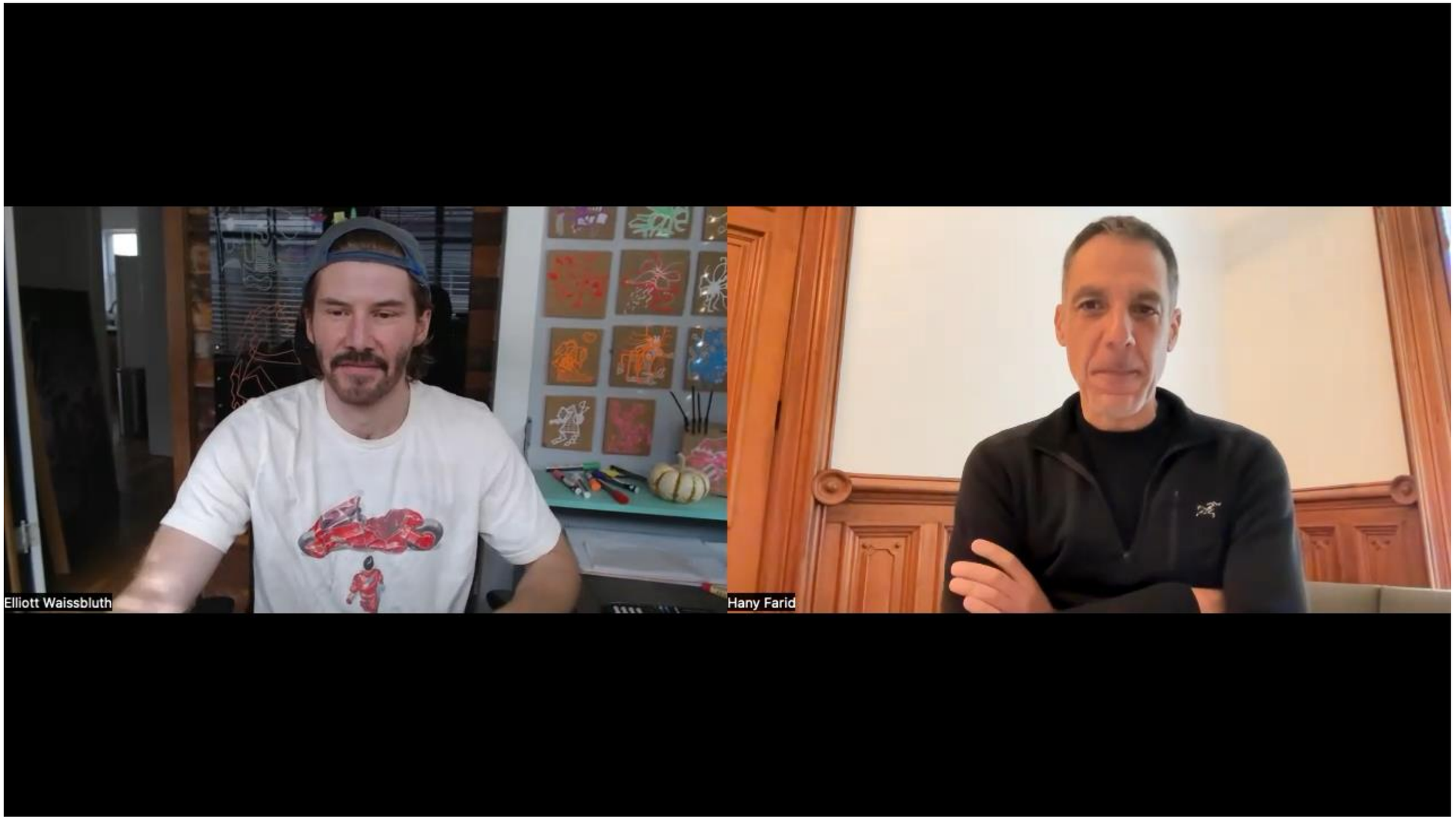
It’s not just Taylor Swift: AI-generated porn is targeting women and kids all over the world

By Samantha Murphy Kelly, CNN

6 minute read · Updated 3:51 PM EST, Fri January 26, 2024

D-Keine/iStockphoto/Getty Images

Real-Time Video



Real-Time Video

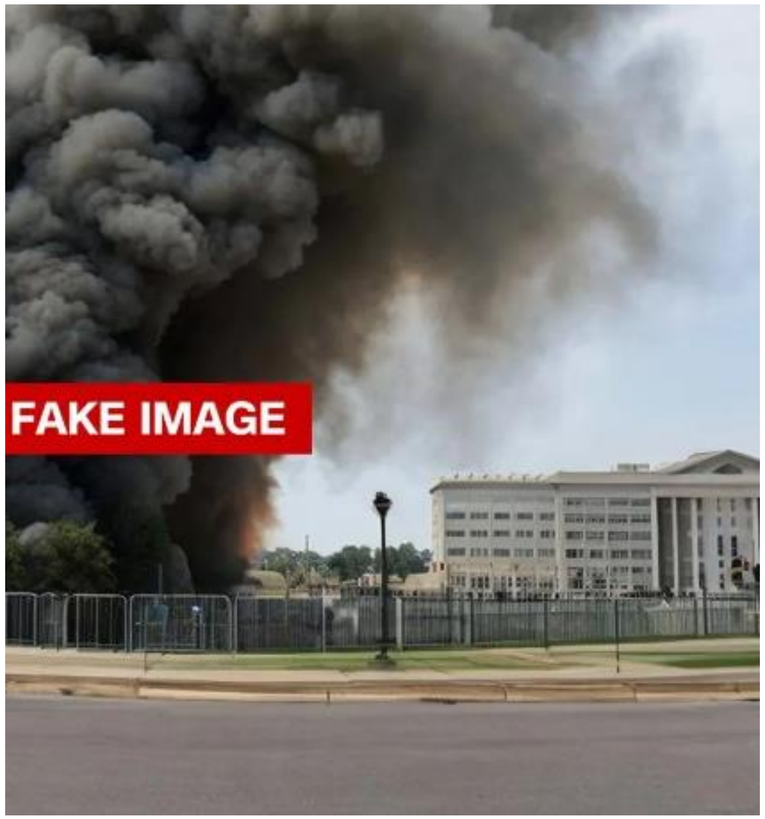
Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

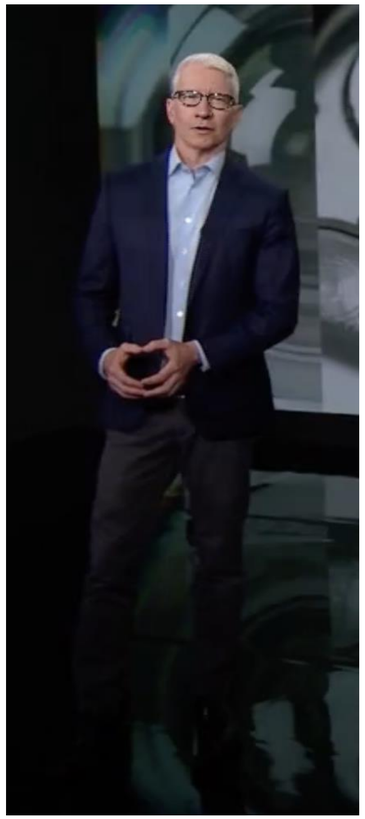
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

Threats



fraud/elections



disinformation

information security

challenges

unprecedented speed of AI
many players from AI-tech to big-tech
open-source models

solutions (legislative)

copyright infringement
choke points:
- financial institutions
- infrastructure

solutions (non-legislative)

proactive (watermark/fingerprint)
reactive (forensic analysis
incentives (model poisoning)

Predictive AI

Machine Learning (ML) ≠ Artificial Intelligence (AI)

The best way to repeat history is to train ML on historical data