## Al and Evidence: Let's Start to Worry

Article By:

Theodore F. Claypoole

When researchers at University of Washington pulled together a clip of a faked <u>speech by President</u> <u>Obama</u> using video segments of the President's earlier speeches run through artificial intelligence, we watched with a queasy feeling. The combination wasn't perfect – we could still see some seams and stitches showing – but it was good enough to paint a vision of the future. Soon we would not be able to trust our own eyes and ears.

Now the researchers at University of Washington (who clearly seem intent on ruining our society) have developed the next level of AI visual wizardry – fake people good enough to fool real people. As <u>reported</u> recently in Wired Magazine, the professors embarked on a Turing beauty contest, generating thousands of virtual faces that look like they are alive today, but aren't.

Using some of the same tech that makes deepfake videos, the Husky professors ran a game for their research subjects called Which Face is Real? In it, subjects were shown a real face and a faked face and asked to choose which was real. "On average, players could identify the reals nearly 60 percent of the time on their first try. The bad news: Even with practice, their performance peaked at around 75 percent accuracy." Wired observes that the tech will only get better at fooling people "and so will chatbot software that can put false words into fake mouths."

We should be concerned. As with all digital technologies (and maybe most tech of all types if you look at it a certain way) the first industrial applications we have seen occur in the sex industry. The sex industry has lax rules (if they exist at all) and the basest instincts of humanity find enough participants to make a new tech financially viable. Reported by the <u>BBC</u>, "96% of these videos are of female celebrities having their likenesses swapped into sexually explicit videos – without their knowledge or consent."

Of course, given the level of mendacity that populism drags in its fetid wake, we should expect to see examples of deepfakes offered on television news soon as additional support of the "alternate facts" ginned up by politicians, or generated to smear an otherwise blameless accuser of (faked) horrible behavior. It is hard to believe that certain corners of the press would be able to resist showing the AI created video.

But, as lawyers, we have an equally valid concern about how this phenomenon plays in court. Clearly, we have rules to authenticate evidence. New Evidence Rule 902(13) allows authentication of records "generated by an electronic process or system that produces an accurate result" if "shown by the certification of a qualified person" in a particular way. But with the testimony of someone who was wrong, fooled or simply lying about the provenance of an AI generated video, the false digital file can be easily introduced as evidence.

Some Courts under the silent witness theory have allowed a video to speak for itself. Either way, courts will need to tighten up authentication rules in the coming days of cheap and easy deepfakes being present everywhere. As every litigator knows, no matter what a judge tells a jury, once a video is seen and heard, its effects can dominate a jury's mind.

I imagine that a new field of video veracity expertise will arise, as one side tries to prove its opponent's evidence was a deepfake, and the opponent works to establish its evidence as "straight video." One of the problems in this space is not just that deepfakes will slip their way into court, damning the innocent and exonerating the guilty, but that the simple existence of deepfakes allows unscrupulous (or zealously protective) lawyers to cast doubt on real, honest, naturally created video. A significant part of that new field of video veracity experts will be employed to cast shade on real evidence – "We know that deepfakes are easy to make and this is clearly one of them." While real direct video that goes to the heart of a matter is often conclusive in establishing a crime, it can be successfully challenged, even when its message is true. Ask John DeLorean.

So I now place a call to the legal technology community. As the software to make deepfakes continues to improve, please help us develop parallel technology to be able to identify them. Lawyers and litigants need to be able to clearly authenticate genuine video evidence to clearly strike deepfaked video as such. I am certain that somewhere in Langley, Fort Meade, Tel Aviv, Moscow and/or Shanghai both of these technologies are already mastered and being used, but we in the non-intelligence world may not know about them for a decade. We need some civilian/commercial help in wrangling the truth out of this increasingly complex and frightening technology.

Copyright © 2025 Womble Bond Dickinson (US) LLP All Rights Reserved.

National Law Review, Volume IX, Number 318

Source URL: https://natlawreview.com/article/ai-and-evidence-let-s-start-to-worry