The Growing Threat of Deepfakes to the Legal Profession

October 27, 2020

Once upon a time, people worried that Adobe Photoshop would enable anyone around the world to create images so lifelike that history itself could be rewritten with just a little experience in graphic design. While Photoshopped or "shopped" images remain a legitimate threat to truth, technology has advanced much further than even the gloomiest of doomsayers could have once imagined. Now, there are software programs that can synthesize voice, audio, video, text, and other forms of evidence, sometimes from thin air or via manipulation of genuine data. These fabrications are known as *deepfakes*.

The legal practice relies upon evidence, and the integrity of the judicial system relies upon the authenticity of that evidence. So how is the profession keeping up? And what role might individual lawyers play in the growing struggle for truth and justice?

A deepfake is, first and foremost, a form of synthetic (artificial) media. It involves taking the image or sound of an individual and replacing it with a highly convincing substitution. Although the concept of the deepfake itself is nothing new, artificial intelligence (AI) and other technological advances are making it easier to create synthetic media – and much more difficult to discern deepfakes from reality. Some have called deepfakes "Photoshops on steroids."

According to a report by Deeptrace Labs, a cybersecurity company, 96% of manipulated videos on the internet are pornographic. But it's no longer just the realm of internet pornography where deepfakes thrive. They are now crossing over into legitimate and mainstream media, as well as other parts of the culture. That includes the practice of law.

In one British child custody case, a woman claimed that her husband was dangerous. What's more, she claimed to have the audio to prove it. But as the husband's attorney was thankfully able to determine, the recording had been manipulated to make it sound like the man was making threats. What's worse, the synthetic media was created using widely available online software programs and instructions.

As it turns out, the recording itself was of relatively low quality. The husband's attorney was able to examine its metadata and, with the assistance of experts, determine it was a deepfake. However, these facts alone pose some troubling developments for the legal profession. To begin with, how many attorneys or judges are really examining data this closely in the first place? And second, will experts – who can cost significant time and money – need to be brought in to every case in which the reliability of data is suspect?

Nothing less than the trustworthiness of evidence, and that of the entire legal system, is at stake as deepfakes grow in ubiquity and sophistication. As such, lawyers and judges will have an important role to play in identifying and stopping the menace posed by synthetic media. Stay tuned for our next post which will give some tips and strategies for combatting deepfakes.