

## All.Net Analyst Report and Newsletter

### Welcome to our Analyst Report and Newsletter

#### Dealing with deep fakes

I have been reviewing articles over the past year or so regarding different issues and came across the “deep fake” meme more than once. I thought it might be worth addressing the deep fake we are seeing about deep fakes.

#### Question: How deep do we need to go?

The first thing that may come to mind is the question of how deep is deep. It’s kind of like “big data”. How big does the data have to be to be called big? I figure anything that takes more than once cubic centimeter per bit is pretty big even by historical standards. But I suspect that’s not what they meant by the term. The “biggest” dataset<sup>1</sup> I ever worked with on a legal matter was about 10 trillion semi-structured records. I think that’s probably bigger than most “big data” things we hear about today.

My point is, how do we measure “deep”? I think the answer for “fakes” (i.e., deceptions) is we only need to go as “deep” as it takes to fool (successfully deceive) the audience long enough for the desired effect (behavioral difference). So to be clear, for the average person looking at Facebook for a quarter of a second to two seconds, not very deep at all. An artist’s depiction is probably good enough.

#### How do we measure “deep”?

In seeking metrics for “deep”, there are no obvious methods. We could measure it with social science by putting “fakes” and “reals” in front of people and measuring their ability to properly discern in a limited time frame with specific conditions. I hypothesize that tools from the 1970s used by people with a week of training would have no problem exceeding the 95% standard for social science for being “effective” fakes for postings to social media of still pictures.

But that is a far cry from fooling, by example, the legal system. In the legal system, any evidence starts the admission process by detailing the provenance. How did it come to be? How did it come to me? What did I do with it? That’s for every step since its initial creation. Missing a step? Likely inadmissible as to its reliability<sup>2</sup> and authenticity<sup>3</sup>. Then the forensic examination. Examiners have long found lots of ways to detect alterations to content. This runs from detecting things that are inconsistent with the real world of physics to detecting that different mechanisms were used in producing different parts of the content. Many have tried and failed to slip one past. How do we measure this? Same method, but far more expensive.

#### Conclusions

The thing about deep fakes is that the term itself is a deep fake. No metrics for depth or fakery have been provided, and as such, it is little more than a spreading malicious meme likely intended to trigger fear to be resolved by paying someone something. So pay me instead, don’t worry about “deep fake” technology, but worry about the people promoting it.

1 For those under 50, “dataset” is an old term for a collection of data. For those under 30, “data” includes anything made up of sequences of symbols. For those ... symbols include, without limit, bits.

2 Reliability in the legal world means, in effect, reflective of reality.

3 Authenticity in the legal world means, in effect, unaltered since initially created.

## Almost... because

The conclusion on the last page was intended to get others (not you) to ignore the rest of the article, because folks who don't look past the obvious deserve to be taken advantage of.

Actually... not. I used the term "because" in the last sentence because it triggers an automatic association and acceptance of the causal relationship. Even if both halves of the sentence may be true, it doesn't mean that the relationship is causal.

You probably think this article's about you.<sup>4</sup> And you can tell everybody – this article's for you.<sup>5</sup> But it's only partly true. Of course the article is about all of us, and if the song wasn't about the person who was vain, who exactly was it about? All symptoms of the our cognitive errors.

## People who intentionally deceive for advantage

In my view, the underlying problem is people who want to take unfair advantage of others. "There's a fool born every minute"<sup>6</sup>, and that was from 1806 – the rate of births is considerably higher today. But in reality, everyone ever born is potentially a fool, because we all make cognitive errors. Indeed mathematical theory tells us that there is no fool-proof system (technically, no system that is both consistent and complete). Ain't a horse that can't be rode, ain't a man who can't be throwed.<sup>7</sup>

The problem, at its core, is the volume of people trying to take unfair advantage of other people. When I say "unfair" I mean to say is that they are taking advantage of the weaknesses of other people to harm the other people and benefit themselves.

## As old as the hills

Exploitation is nothing new. The scalability of information technology is nothing new. In 2001, I was given an award for some of my work in digital forensics and asked to give a talk at a conference on digital crime investigation. At that same conference I also gave a presentation on the future of digital crime. I said, in essence, all of the technology used to gain efficiencies for business are going to be used for criminal efficiency as well. I gave examples of big crime (like big business). The two edged sword of technology is sharp on all sides. We should, have, and continue to anticipate that bad people will use technology to do bad things.

## Conclusion

The problem of "deep fakes" is that people keep trying to push them to take advantage of other people. Technology people tend to do things without thinking of the ethics of it. The major technical societies have ethics standards and guidelines that are widely ignored. Better entertainment justifies better video production. But what exactly justifies intentionally creating automated deceptions that makes it look like real people said things they did not say? What justifies doing it at high fidelity? What is the ethical or other benefit of this to society? How does it benefit anyone? Stop throwing bigger rocks at windows to try to force people to get stronger windows. Stop supporting those who do this. And stop pushing the fear button.

---

4 Homage to Carley Simon

5 Homage to Elton John...

6 Per "<https://quoteinvestigator.com/2014/04/11/fool-born/>" In 1806 an article titled "Essay on False Genius" was published in "The European Magazine and London Review"... "That there vash von fool born every minute." - attributed to the tribe of Levi.

7 Old West saying without a good source – I used it in my dissertation to the chagrin of the copy editors who indicated it weren't good English.