Published April 18, 2024. Editor's Headline: Getting Smarter About Artificial Intelligence.

https://www.thecheyennepost.com/opinion/columnists/getting-smarter-about-artificial-intelligence/article_772a772e-fdac-11ee-8d30-bbb6e9d8ed11.html

Artificial intelligence (AI) has been touted as a great advance but, like so many "improvements" of modern life, it is also a deal with the devil.

"Learning Deep Learning" is the title of a technical publication I came across when I visited California. Silicon Valley is home to any number of companies and conferences that specialize in artificial intelligence (AI) products.

A chart in the book shows that deep learning (DL) is embedded in machine learning (ML), which is embedded in AI. In turn, deep learning hosts deep neural network (DNN) as embedded in it.

The book comprises some 630 pages. Put together by a software architect and ESL writer, it's hard to follow at times; still, my interest was piqued by a heading in the Preface, "Is DL Dangerous?" Here is my paraphrase:

Unintended Consequences:

> A 2018 study by Buolamwini and Gebru centers on a facial recognition system used by law enforcement. While the system achieved 99% accuracy on lighter-skinned men, its accuracy on darker-skinned women was only 65%, putting them at risk of being misidentified and wrongly accused.

The system remains "commercially available."

Malignant Use:

> A 2019 study on fake pornography by Dickson found that the technology is used to make it appear as if a person, often a celebrity, is featured in a pornographic video.

In other words, AI is saddled with both unintended consequences and malignant use. That these studies were done four and five years ago tells us, these iniquities have been going on for a decade or more although, over the past few years, ethical AI has become a significant area of focus.

The author notes that "DL learns from data created by humans and consequently runs the risk of learning and even amplifying human biases." While he mentions the "need for taking a responsible approach to DL and AI," he acknowledges that, historically, "this topic has largely been neglected." He draws attention to the website of the Algorithmic Justice League that has raised the alarm—but the horse is out of the barn, isn't it?

A foreword by Dr. Anima Anandkumar touches on the topic also. While her writing, too, suffers from long-winded prose, the gist of it says, it's paramount that every AI engineer "think critically about the societal implications around the deployment of AI." The author points to the proliferation of harassment, hate speech, and misinformation in social media that "wreaks havoc" in society. She adds that

> Groundbreaking studies such as the Gender Shades Project and Stochastic Parrots have shown highly problematic biases in AI models that are commercially deployed at scale.

Anandkumar says she has advocated for banning AI in the use of facial recognition by law enforcement until "appropriate guidelines and testing are in place." The question is: who will design and implement the guidelines?

Meanwhile a glance at internet news yields headlines like, **Voice deepfakes are calling — here's what they are and how to avoid getting scammed:** Powerful AI tools available to anyone with an internet connection make it easy to impersonate someone's voice, increasing the threat of phone scams.

The authors represent the DeFake Project at the Rochester Institute. Professor of Computing Security Matthew Wright, and Research Associate of Computing Security Christopher Schwartz, point to chatbots like ChatGPT that generate realistic scripts with adaptive real-time responses. "By combining these technologies with voice generation, a deepfake goes from being a static recording to a live, lifelike avatar that can convincingly have a phone conversation." The researchers explain

> For starters, voice phishing, or "vishing," scams are the most likely voice deepfakes. . . . In 2019, an energy firm was scammed out of US$243,000 when criminals simulated the voice of its parent company's boss to order an employee to transfer funds to a supplier. In 2022, people were swindled out of an estimated $11 million by simulated voices, including of close, personal connections.

Do not rely on caller ID, warn the researchers; these can be faked. Further, be careful with your personal identifying information. Your Social Security number, home address, birth date, phone number, middle name—even the names of your children and pets—can be giveaways for scammers to impersonate you to banks, realtors, and others.

Another headline reads, **AI hustlers stole women's faces to put in ads. The law can't help them.**

Nitasha Tiku of the Washington Post explains that AI has created "a new type of identity theft." Ordinary people find "their faces and words twisted to push often offensive products and ideas." Tiku gives an example:

> The 27-year-old content creator was with her husband in a rented cabin in snowy Maine when messages from her followers began trickling in, warning that a

> YouTube commercial was using her likeness to promote erectile dysfunction supplements.

The commercial showed her in her real bedroom, wearing her real clothes but describing a nonexistent partner with problems in bed. Scammers appeared to have stolen and manipulated one of her videos by using "a new wave of artificial intelligence tools" that can create realistic "deepfakes," a catchall term for media altered (or created) with AI.

Because it's simpler and cheaper to base fake videos on real content, grifters scoop up videos on social media that match the demographic of a sales pitch, "leading to what experts predict will be an explosion of ads made with stolen identities," says the author.

On April 9, 2024, an open letter signed by over 200 big names in the music industry was posted by a nonprofit musician advocacy group on Medium: **How musicians are fighting AI for fair wages.** The letter pleads with AI companies to not use the technology to devalue their music.

> "Unchecked, AI will set in motion a race to the bottom that will degrade the value of our work and prevent us from being compensated for it," says the letter.

Earlier this year, on January 30, 2024, Universal Music Group moved against AI when it pulled its entire catalog off of TikTok, which has been plagued with the infringements that artists are fighting against. An open letter to the Artist and Songwriter Community bore the headline, **Why We Must Call Time Out on TikTok.**

> TikTok is allowing the platform to be flooded with AI-generated recordings—as well as developing tools to enable, promote, and encourage AI music creation on the platform itself—and then demanding a contractual right which would allow this content to massively dilute the royalty pool for human artists . . . [it] is nothing short of sponsoring artist replacement by AI.

"This hurts," a musician told me. "We can no longer use TokTok to promote our music." Musicians' margin of profit is already thin, he said, and some AI tactics make it disappear altogether.

"Hollywood actors are hurting as well," he said. "Where formerly they earned a smidgen whenever they appeared as extras in a crowded film scene, today, they're being replaced with clones."

Meanwhile, a Google search of "phishing" shows an astounding variety of posts, from cyber-security companies offering their services to advice posts like "How to Recognize and Avoid Phishing Scams."

You'll learn that imposter scams are extremely common in the United States. A few years ago, scammers siphoned $98 million from Facebook and $23 million from Google by sending fake invoices to employees.