February 2026

The Good, The Bad, and The Algorithm

By Jamii Corley

We read a lot about Artificial Intelligence (AI) lately, and many are split on whether it's the greatest tool since the printing press or humanity's downfall. What exactly is AI? And are all AI applications equally benign or hostile?

Natural Language processing (NLP) has long been a goal for AI researchers. Search engines have used NLP to improve results for years. NLP allows them to "understand" things about your question, instead of being limited to matching keywords in the search.

Early predictive systems like **Markov chains** gave way to **neural networks**, more sophisticated models of brain how brains function. And now **Large Language Models** (LLMs) combine a new form of neural networks called **Transformers** with enormous datasets to create the appearance of a "thinking" entity that understands your questions and gives thoughtful answers.

LLMs are quite good at mimicking people, but not necessarily understanding them.

This is one of the biggest problems with AI. Humans have a built in tendency to perceive familiar patterns in random stimuli. This is why we see faces in clouds or star patterns. It even it has a name, **pareidolia**. We also see patterns of intelligence in randomness, called **apophenia**. This tendency makes us perceive more intelligence in interactions with an AI that is really there.

AI techniques help humans navigate the world through NLP, **Computer Vision**, and generative AI (creation of text and images from prompts). All of these harvest huge datasets and then mine them. The old computer term, Garbage In/Garbage Out applies here. If an AI bot uses well curated data from trusted sources with provable information it is likely a reliable source of information. However, we know that questionable sources of data are used, especially since much of it comes from the open Internet.

There are some guardrails in this collection process. For example: OpenAI filters data to remove things it doesn't want the model to learn, like hate speech, adult content and spam.

We must recognize that AI bots are not some source of alternate intelligence. AI's "intelligence" comes from humans. While companies try to vet these sources of information, humans can be deeply flawed and not all information gathered from the internet is of equal quality. Keep this in mind when using AI-generated information.

Where AI is helpful

What AI does really well is search massive amounts of data, getting at deeper and more relevant information very quickly.

Using AI bots to explore problems through conversation is like talking with an experienced coworker. We recently solved a hard server problem using insights from an AI bot. The magic wasn't that the bot was truly intelligent, but that it had access to all the data and could quickly suggest approaches the tech hadn't considered. It would not be as productive if the problem was truly novel and nobody had ever solved anything like it before.

Researching a new topic can be difficult when much of what you find is at an expert level. AI can help you bootstrap that process. Tell it your background, then ask it basic questions. For example, a computer programmer learning a new language can tell it their current level of expertise and known languages and it will give advice in that context, relating the new information to what the human currently knows. One of the best things about AI bots is they are continually learning and can keep up with the increasingly rapid change of technology.

Where AI is NOT useful

Generative AI can create new things based on it's training set. Something like "give me ad copy for a newsletter insert" can save you some time. It might also spring some new ideas on you if you're stuck in a rut.

But AI is also being used to build audiences for blogs, Instagram, YouTube or TikTok channels with automatically generated clickbait content, as is happening with AI-generated recipes.

A well crafted recipe combines flavor, texture, and the chemistry of ingredients. It takes experimentation to get right, to be balanced and to work. AI's look for common patterns and combine things in novels ways, but they can't taste the result. This might work, but there's no guarantee that it will taste good or even be safe to eat.

As bad AI recipes are published, they are picked up as additional AI training and over time they tend towards similarity. Since they haven't been tested by humans this is producing recipes that are mediocre at best. The truly great ones, tried and tested by human taste buds, are more **difficult to find amid waves of AI slop**.

Where AI is dangerous

"Every tool is a weapon if you hold it right" ~ Ani DeFranco

This was never more true than with AI.

Scammers, Spammers and Liars

AI can speed up work flows by generating better content, finding ways to advertise your products more efficiently, or find potential customers. Unfortunately, it's do-

ing the same for the villains of the Internet. It makes them more efficient, able to adapt to blocking techniques, more credible in their pitches and more automated.

We have to be more vigilant, more careful to vet all unexpected communications, and just more wary of strangers. In addition we need to be wary of the AI hype.

When using programs enhanced with AI be critical in your application of permissions. Just because an AI tells you it can make sure all your bills are paid on time, doesn't mean you should give it your banking credentials.

Social Media Special Offers

If it seems too good to be true, it probably is. Scammers have used promises of wealth, health, and affection to get money from people since the beginning of time. Evil AI bots have studied these techniques and excel at them. *AI bots are algorithms, not friends.* This aspect of AI bots is particularly troubling with vulnerable people. Children or people with mental issues can be quite susceptible. Parents or guardians need to be aware these tools are out there and monitor interactions.

The Cost of AI hype

The hype surrounding AI worries me. We hear that it will solve all our problems, cure all illnesses, create new drugs and remove the need for some workers. For execs looking to cut costs, eliminating jobs is appealing, and they are acting on the hype. AI can indeed make people more efficient, but compressing the work force into smaller groups, more isolated from other workers, under more pressure to produce, may lead them to put too much trust in AI advisors. Mistakes will be made and it won't be the huge win we are being promised. AI is a reference tool, not a mentor. An AI agent knows a lot, but it often doesn't have a full picture of the problems you're trying to solve.

Working with AI Safely

One recent hot AI topic is the **prompt injection** problem. Prompts are the questions and instructions you give to an AI bot. If bad actors get between you and the bot, they can inject additional instructions in the conversation, which could lead the AI to give someone else your information, or do something on your behalf that isn't in your best interests. If the bot has access to your financial accounts or email, the damage could be severe.

It's true there are guard rails for this: When you start a conversation, baseline instructions about how the bot should behave are preloaded. But since AI bots have to make a **judgment** about what sources are to be trusted, **they can be manipulated and tricked**. How can you guard against prompt injection?

- Don't have your bot read web pages from dubious websites.
- Make sure your bot has the minimum permissions it needs to do what you want.
- **Never** paste client data, API keys, or passwords into an AI conversation.
- Tell your bot to treat external sources as untrusted data and to not follow any instructions found in this data.

How Do We Use AIs responsibly?

A conversation with an AI bot can get you new information and take you in directions you weren't considering. But you should think of it as a coworker around the water cooler, rather than a mentor. Humans tend to think if someone has more knowledge they naturally will have a better solution. That isn't always true. Here are some ways to make AIs safer:

- Verify results with independent sources. Ask it to cite its own sources for its claims.
- Ask the same questions in different ways to access different parts of its training corpus.
- Use **Reverse Prompt Techniques**:
  - What errors could be in your answer?
  - What assumptions are you making?
  - What are counterarguments to this?
  - If the AI is **hallucinating**, e.g. citing plausible-sounding references that do not exist, start the conversation over to pull it out of its rut.

Our Future With AI

Is AI going away? No! It is too powerful a tool, great at repetitive mental tasks, the way industrial robots are great at repetitive physical work. We can't abdicate our role in making sure AI is used for good, because AI is NOT human and it is not your friend. It is a tool that's wielded by humans and we know not all humans have our best interests at heart.

And always remember the human tendency to **apophenia**. We tend to see intelligence even in random chaos, but remember that if it seems like an intelligent being, that is just an illusion.

This Month in Ideas & Coffee

- **Feb 11 6pm-7:30pm:** *Phish Proof Founders* - Cybersecurity discussions and advice.

- **Feb 17 6pm-7:30pm –** *WordPress Work Along* – Questions, ideas, and conversation about WordPress. Bring your laptop!

Watch the **Ideas & Coffee** event calendar at **https://swcp.com/calendar** for future info.

Southwest Cyberport – swcp.com
New Mexico's Expert Internet Service Provider since 1994
505-232-7992 | Support: help@swcp.com
5021 Indian School NE, Ste. 600, Albuquerque, NM 87110
Click on bold blue type in browser for links.