Dec 29, 2019, 01:00am EST | 50,520 views

Ethical Concerns of AI

Kathleen Walch Contributor
COGNITIVE WORLD Contributor Group
AI

GETTY

Artificial Intelligence is seen by many as a great transformative tech. Will AI systems one day drive us around? Do our laundry? Mow our lawn? Raise our kids? Fight wars? Write these articles? Create political advertisements? These questions make people shift from thinking purely about the functional capabilities to the ethics behind creating such powerful and potentially life-consequential technologies. As such, it makes sense to spend time considering what we want these systems to do and make sure we address ethical questions now so that we build these systems with the common good of humanity in mind.

Will AI replace human workers?

The most immediate concern for many is that AI-enabled systems will replace workers across a wide range of industries. AI brings mixed emotions and opinions when referenced in the context of jobs. However, it's becoming increasingly clear that AI is not a job killer, but rather, a job category killer. As has happened with every wave of technology, from the automatic weaving looms of the early industrial revolution to the computers of today we see that jobs are not destroyed, but rather employment shifts from one place to another and entirely new categories of employment are created. We can and should expect the same in the AI-enabled economy. Research and experience is showing that it's inevitable that AI will replace entire categories of work, especially in transportation, retail, government, professional services employment, and customer service. On the other hand, companies will be freed up to put their human resources to much better, higher value tasks instead of taking orders, fielding simple customer service requests or complaints, or data entry related tasks.

Indeed, the move to this new age of digital transformation is creating concerns about labor displacement, with or without the power of AI. All AI is doing is hastening digital transformation across particular business processes. As companies are looking to adapt and implement AI strategies we think it's important to have open and honest conversations with your employees. In particular, experience and research is showing that companies that adopt augmented intelligence approaches, where AI is augmenting and helping humans to do their jobs better, rather than fully replacing the human, not only shows faster and more consistent ROI for organizations, but also is welcomed much more warmly by employees. People feel more comfortable working with machines instead of being replaced by machines.

The rise of fake media and disinformation: Will AI make this worse?

AI systems are getting really good at creating fake images, videos, conversations, and all manner of content. We already have trouble believing everything we hear, see, and read. What happens when you can no longer tell if an image is real or AI-generated or if you're talking to a bot or a real person? It's been widely reported that bots had a role to play in the 2016 US Presidential elections spreading political propaganda. These automated social media accounts helped create and spread misinformation on the internet attempting to manipulate voters and fueling the fire of partisan disagreement. Unlike humans, bots never tire working 24/7 and can generate a very large amount of content in a very short period of time. Once shared and re-tweeted with others this news starts to go viral, true or not, and is virtually unstoppable. These bots are effective at spreading false or heavily altered facts, amplifying messages, and putting thoughts and ideas into people's heads. Criminals and state actors can use fake imagery or audio to cause personal or business harm or to interfere with government operations. Now all it takes is a few malicious actors spreading false claims to traumatically alter public opinion and quickly shift the public's view.

Governments and corporations alike will have to think about how they will reign in the potential damage done by AI-enabled content creation. In fact, we encourage companies and governments to consider fake content to be as malicious as cybersecurity threats and respond appropriately. Propaganda, disinformation, malicious interference, blackmail, and other forms of "information crime" can be just as harmful as physical and electronic attacks on systems. The world is very much unprepared for AI being unleashed on unprotected citizens. Corporations who freely traffic in user-generated content are just as liable as governments to curb abuse.

MORE FOR YOU

The Energy Transition Must Lay A False Dilemma To Rest

Can AI Help Us Manifest The Life We Want? A Discussion At The Intersection Of Mindset And Machine Learning

Want To Boost Your Returns From AI? Follow The Leaders

Do we want evil people to have easy access to AI technology?

While AI can do a lot of good we must be mindful about AI in the hands of malicious users. As technology continues to become more powerful, AI can cause severe damage if used maliciously. What happens when individuals, criminal organizations, and rogue countries apply AI to malicious ends? Many companies are already asking themselves these questions and starting to take action to safeguard against malicious AI attacks. New technologies can exploit the vulnerability of systems that are dependent on AI and machine learning technologies. As these AI systems get smarter they can change the nature of threats, making them harder to detect, more random in appearance, more adaptive to systems and environments, and more efficient at identifying and targeting vulnerabilities in systems. This should be terrifying. We need to immediately start thinking about how we are constructing and managing our digital infrastructure as well as how we design and distribute AI systems. Detecting these malicious attacks will only get harder over time.

In addition, machine learning service providers, especially on-demand cloud-based services should be mindful of who their customers are. If malicious users are using their platforms to perform distributed AI-enabled attacks or other criminal acts, then like financial institutions, governments will start cracking down on these providers and impose new forms of "Know Your Customer (KYC)" regulations. If these platform providers don't want to be on the wrong end of the regulatory cycle, they need to get ahead of the curve and start their own efforts to make sure they know who their customers are and what they are doing on their platforms.

Is pervasive surveillance already here? Is AI our new Big Brother?

AI enables companies and governments to keep constant tabs on what humans are doing in an automated and intelligent fashion. Will a future with AI mean an end to privacy? Will "Big Brother" really always be watching? As facial recognition technologies continue to advance it's getting easier to detect individuals from a large crowd of people at stadiums, parks, and public spaces without their permission. In 2018 Microsoft urged Congress to study it and oversee the use of facial recognition technology. Bradford Smith, the company's president said "We live in a nation of laws, and the government needs to play an important role in regulating facial recognition technology". What's striking about this statement is that tech giants rarely advocate regulation of their innovations, so for Microsoft to be urging the US Congress to regulate facial recognition they must already see how this technology can be misused.

In an AI-enabled future we assume that everyone and everything will have knowledge about everyone else. This means that the assumption will be that everyone already knows who we are, what we want, where we are, and what we're doing. This pervasive knowledge will become part of the assumption of where we are, just like we are now expecting to be able to get Internet, electricity, and information whenever and wherever we need it without excuse. No longer will we be able to just "un-plug" for a while. We may quickly move to a world where just a few companies and government have an uncomfortable amount of knowledge and level of control over the lives of everyone.

Will intelligent machines have rights?

As machines become more intelligent and we ask more and more of our machines, how should they be treated and viewed in society? Once machines can actually simulate emotion and act similar to human beings, how should they be governed? Should we consider machines as humans, animals, or inanimate objects? To this point, to what level do we ascribe liability and responsibility to the devices themselves over the people that are supposedly

in control of them? In March 2018 an autonomous vehicle struck and killed a pedestrian. People were outraged that a machine killed a human being.

But why were people outraged by this accident? Thousands of people are killed every day in motor vehicle accidents caused by humans at the wheel. What difference should it make that it was a machine driving the vehicle? The reason for this outrage is because society hasn't, and may never accept, when a machine kills a human. However, the likelihood of eliminating all traffic-related fatalities is almost certainly zero percent. As such, if we want autonomous vehicles on the road this scenario will happen again, and again. Despite perhaps dramatic evidence that machine-driven vehicles have overall far lower fatality rates than human-driven vehicles, the issue of liability and control is primarily one of ethics. So we need to be asking these questions, figuring out what we can accept and what's ethical, and put laws and regulations in place now to safeguard against future tragedies.

Creating transparency in AI decision-making

There are many approaches used in machine learning, however, no machine algorithm has re-invigorated the AI market quite like deep learning. Deep learning, however, is a "black box". We aren't really sure how deep learning works and this can be a big problem when we rely on this technology to make critical decisions such as loan applications, who gets paroled, and who gets hired. AI systems that are unexplainable should not be acceptable, especially in high risk situations. Explainable AI needs to be part of the equation if we want to have AI systems we can trust.

Deep learning relies heavily on training data. So it should be no surprise then that when biased training data is used to teach these systems the results are biased AI systems. People wrongly assume that the training data is always "clean", from a large pool, and represents society as a whole but results have proved this is not the case. Google's image recognition system wrongly classified images of minorities, the Apple Card which is administered by Goldman Sachs has come under recent scrutiny for gender

bias, and software used to sentence criminals was found to be biased against minorities. If we are going to use machine learning algorithms to make any sort of worthwhile decision we must demand that it be able to explain itself. Would you really allow a human driver to hit your car and when you question why they did that they have no answer? Of course you wouldn't. We shouldn't accept this from machines either!

Taking steps to resolve these issues

If we don't ask ourselves these questions now and build ethical AI, implications down the road can be far more grim than people realize. Do we really trust companies to do the right thing? Do we trust governments to do the right thing? We'd like to think that with public input and ethical questions and concerns brought up now, that we can create a future that isn't so grim. There will always be bad actors who try to influence, infiltrate, and manipulate. Enterprises, organizations, and citizens should keep asking questions, keep working towards building ethical AI, and keep trying to fight automated bots and malicious attacks because AI is coming whether or not we're ready.

Follow me on Twitter. Check out my website.

Kathleen Walch

Kathleen Walch is Managing Partner & Principal Analyst at AI Focused Research and Advisory firm Cognilytica (http://cognilytica.com), a leading analyst firm focused on...

Read More