- Home
- Understanding the Risks Associated With AI

# News

- Print
- Download PDF

# Understanding the Risks Associated With AI

11 Mar 2019

Expert explains the difference between the weak and strong types

Artificial intelligence has been variously depicted as a universal panacea for the world's ills or as a conspiracy by deep-state operatives. AI's influence is everywhere, yet there is much that remains unknown about its practical applications and its long-term potential.

To get a better understanding of what AI is, let's start with the basics. Historically, AI was a way of designing algorithms that could, in some limited sense, mimic human intelligence. In its infancy, AI's practical applications

extended little more than the development of computer programs that could prevail in chess matches against people.

Over time, the technology has advanced, and now there are two types of AI: weak AI and general or strong AI.

Weak AI is basically a program designed to accomplish a specific task, such as a vacuum cleaning floors on its own or a car driving autonomously.

General or strong AI involves designing a program to replicate a multifunctioning human that can complete several tasks depending on the situation.

The majority of recent innovations involve weak AI, and there are some theoretical insights that suggest that, perhaps, general or strong AI is impossible.

Even so, we already use AI technology in almost every aspect of our lives. Some elements of AI have been used to make better predictions and data more easily available. When we upload pictures of friends on Facebook, for example, the site recognizes those pictures. When we use Google's search engine or its maps app, or shop on Amazon, those companies take note. Therefore it is important to understand the associated benefits and risks.

AI has the potential to compartmentalize information, so that we see only things that the program thinks we are interested in, and therefore doesn't suggest other items for us to explore. If, for example, you buy a book about gardening on Amazon, the website's recommendation system will suggest more books to buy on the same subject, even though you might be looking for a cookbook the next time you visit the site. This wouldn't be the case if you were browsing the shelves of a brick-and-mortar bookstore, where you might come across something interesting that you had not considered before.

Another challenge associated with AI is that masses of data are being collected about us—known as big data. Our daily routines are being tracked, to varying degrees. The global proliferation of closed-circuit TV cameras used in cities, for instance, means you are likely to appear on a CCTV camera several times a day.

Because we tend to spend so much time online, our habits and preferences are readily identifiable through so-called weak AI. Google Maps, for example, can learn what time you travel every day, potentially identifying the address of your home and workplace, how long it takes you to commute, and whether you took a detour.

And, of course, through smartphones—the essential accessory of modern life— all our activities can be logged and assessed. Depending on who owns the data, there is the potential for us all to become part of a surveillance society.

## LIMITATIONS

A common test for a machine-learning system is to try to distinguish between an image of a cat and a dog. The AI function is trained to learn the difference—often with high accuracy. However, if just a few pixels in a dog image are altered—which is imperceptible to humans—the system often will start identifying dog images as cats. Thus, contemporary AI is far from foolproof. When it comes to sensitive services, like a nation's defense system, it is important to recognize the technology's limitations.

Having said that, AI is becoming increasingly efficient, particularly from a predictive perspective, though the predictions often misinterpret nuanced information. The facts can be established, but the "How" and "Why" are more difficult to determine.

Despite AI's advancements, we should remember that the technology has limits, and that the sci-fi dream (or nightmare) of strong or general AI remains elusive.

## PRIVACY CONCERNS

In an effort to stem the loss of citizens' privacy, governments are increasingly stepping in, attempting to enshrine into law the right of individuals to opt out of the data-collection epidemic.

Last year the European Union introduced the General Data Protection Regulation, which ensures that website visitors decide whether to have their information stored through cookies.

Ultimately, it is the responsibility of governments to establish a framework that protects the right to privacy, but this aim is difficult to achieve in practice, given the rapidly advancing tech innovations that can get around such restrictions.

At the Qatar Computing Research Institute, part of Hamad Bin Khalifa University, we are drafting a white paper that contemplates the steps governments need to take to respond to AI's advancement.

Ultimately, technological advancement has been at the heart of human progress since the invention of the wheel. And, with progress, challenges are inevitable. AI has the potential to revolutionize our day-to-day existence, but it is difficult to predict where the revolution will take us.

Sanjay Chawla is research director of data analytics for the Qatar Computing Research Institute at Hamad Bin Khalifa University. Several of his papers have been published in the IEEE Xplore Digital Library.

Source

**Tags:**

- Artificial intelligence
- AI
- Privacy Concerns