Artificial intelligence—between scientific, ethical and commercial issues

April 9 2018, by David Glance

On March 18 in Tempe, Arizona, an Uber self-driving car struck and killed Elaine Herzberg, who was walking her bicycle across a street. The human driver was supposed to be monitoring the car's behaviour, but did not do so. Its systems apparently did not detect the victim, as it neither slowed down nor tried to avoid hitting. Credit: Herzberg Wikimedia

The fatal crash involving an autonomous car operated by Uber in the United States was a tragic but timely reminder of the dangers of companies rushing to implement artificial intelligence to be first to market.

At the time of the crash, the driver who should have been ready to react in just such an event as this was looking down. The car itself had apparently failed completely to see the pedestrian and didn't slow down or try to avoid hitting her.

Real-world testing, and risks

Again, we are seeing a technology being principally tested to work under normal conditions so that it can be rolled out to market and not necessarily being built with safety as the primary focus. As the former developer of Uber's machine learning and AI platform has said, car companies should be training their cars in simulated environments which can be programmed to train them in how to detect and avoid any number of possibilities of random events that the car could encounter on the road.

Machine learning suffers from a fundamental problem in that its ability to carry out a task depends on data that is used to train it. What exact algorithm it ends up using to fulfil its eventual purpose and what features are the most important is largely unknown. With deep learning, the multiple layers that make up the overall neural network of the machine learning software make this process even more mysterious and unknown.

We do know that machine learning software picks up biases in the data that is used to test it. Software that is used to calculate the risk of an offender committing a future crime and used frequently by courts in the US has been demonstrated to systematically calculate a significantly lower risk for white offenders than people of colour. Other researchers have shown that machine-learning algorithms learn gender biases that are inherent in the texts that are used to train them.

The dangers of now knowing how things work have been clearly demonstrated by Facebook's recent admission that it really didn't know

what people were doing with data of millions of its users that Facebook had encouraged them to take. With the use of its platform for the spread of targeted fake news during the US presidential election, Facebook again admitted that it hadn't realized that foreign governments would exploit this naivety to undermine democracy.

More than just Facebook

It would be wrong to single out Facebook for being the only company who didn't know their software could be exploited to harm individuals and society. The "right to be forgotten" amendments to data-privacy legislation and enacted by the European Union was formulated specifically to deal with Google's unwillingness to fix side effects of its search on the privacy of individuals. Legislation in many countries to make reporting of data breaches mandatory has been necessary because companies were unwilling to take cybersecurity, and the protection of their users' data, seriously.

Given the past, there is no reason to believe that companies who are implementing systems based on AI are thinking of security and privacy by design. On the contrary, machine learning needs data, lots of it, and so companies are acquiring huge data repositories of detailed information in order to exploit it through algorithms. Whilst one could argue that handled responsibly, large amounts of data will be invaluable for research, in health matters in particular, the risks of collecting, storing and using that data, especially in a commercial setting are very high.

French government report

In France, Cédric Villani – the Field Prize–winning mathematician and member of the National Assembly – has delivered his final report

detailing a national strategy for the study and exploitation of artificial intelligence. The recommendations cover many of the potential issues that could arise from trying to balance the demands for research, innovation and commercialisation of AI. They also recognise the need to safeguard society and individuals' privacy and safety and suggests an active role for government in making sure that AI is used in a way that benefits society and respects human rights and values.

However, none of this will be easy. There has already been claims that Europe's General Data Protection Regulation (GDPR) coming into full effect on May 25, will put EU "firms at a competitive disadvantage compared with their competitors in North America and Asia."

One must hope that tragedies like the death of 49-year-old Elaine Herzberg, run down by a self-driving Uber car, and the widespread outrage of Facebook's disregard for its users' personal data will remind people that there is a benefit to measured technological progress and not today's mantra of technological advancement at any price.

This article was originally published on The Conversation. Read the original article. This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Artificial intelligence—between scientific, ethical and commercial issues (2018, April 9) retrieved 26 April 2024 from https://phys.org/news/2018-04-artificial-intelligencebetween-scientific-ethical-andcommercial.html