

Special Report **50 Ideas to Change the World****Artificial Intelligence and Robotics**

Neural networks allow us to 'read faces' in a new way

Facial analysis software is being used to predict sexuality and security risks



Deep neural networks are making facial recognition software significantly more accurate © Getty
Joshua Jacobs YESTERDAY

Last September, Stanford professor Michal Kosinski unleashed a torrent of controversy when he used artificial intelligence to attempt to [predict peoples' sexual orientation](#) from their faces. Now he has set himself the challenge of deciphering his subjects' political beliefs with similar software.

The research is an illustration of what can be done with deep neural networks — the type of machine learning behind much artificial intelligence, which spots patterns and makes predictions from large volumes of data such as text and images. Other image recognition technologies driven by neural networks are being developed for uses including reading signs for autonomous driving and automatically detecting weapons in airport security scanners.

Neural networks have also made technologies like facial analysis significantly more accurate in recent years. "I'm trying to tell the public that [facial analysis technologies are [already] being used by companies and governments to invade privacy at an unprecedented scale," Prof Kosinski says.

Last summer, Chinese companies began trialling facial recognition software to help police [predict crimes](#) before they happen. Faception, an Israeli company, sells facial analysis software to governments for security uses.

Prof Kosinski and his co-researcher, Yilun Wang, used a facial analysis software called [VGG-Face](#), designed by researchers at Oxford university. Andrea Vedaldi, one of three Oxford

researchers who designed VGG-Face, says that the software's accuracy rate has roughly doubled in the last two years.

Prof Kosinski and Mr Wang extracted data from about 35,000 headshot photos taken from a US dating website, translated their attributes into a sequence of numbers using VGG-Face, and then used a computer model to look for correlations between sexuality and facial features.

When given five photos of each person, the model accurately distinguished between gay and straight men — where one was gay and one was not — 91 per cent of the time and between lesbian and straight women in 83 per cent of cases. When given only one photo of each person, the model distinguished between gay and straight men with 81 per cent accuracy and with 74 per cent accuracy for women — compared to 61 per cent and 54 per cent, respectively, when humans tried the same task.

The authors acknowledge that they have not created a fool proof "Gaydar" that can be applied in the real world — nor do they wish to. Limitations include the fact that they only used images of Caucasians and that their model's accuracy dropped significantly when given other tasks, such as ranking the most likely to be gay among 1000 randomly selected men.

Some are sceptical about the results. Prof Vedaldi says it is conceivable that "what they are showing is true" but questions whether "this has proven in a definite matter that it's actually possible" to detect sexual orientation from faces with neural networks. "Maybe in the database there is some unwanted bias, that would not exist if they were to collect data in some other ways."

Neural networks are very good at spotting patterns, but they're not good at telling you when whether there is actually a correlation

Marta Kwiatowska, Oxford university

"Neural networks are very good at spotting the patterns," says Marta Kwiatowska, an Oxford computer science professor researching their safety risks in self-driving cars. "But they're not good at telling you when they give you [an answer] whether [there is actually a correlation] — because they may be seeing something in a pattern that is random."

Prof Kosinski says that spurious correlations are "the biggest risk" and the "main challenge" with his research. He gives a hypothetical example that could affect the findings for his next project: "It might be

that Republicans tend to take pictures [of their faces] outdoors and Democrats indoors, and there would be a difference on the brightness level." In this scenario, the neural network could focus on brightness rather than facial cues, but would appear to have spotted facial links.

Similarly, it is unclear how exactly his software looked for signs of sexuality and whether it found intrinsic facial characteristics that correlated with sexuality or if it focused mainly on more superficial points such as grooming. Prof Kosinski says that the model looked at both fixed features such as nose shape and more transient factors such as expressions.

“It would be nice to understand if the network can tell you why it thinks the answer is one way or another,” says Prof Vedaldi. “The machine itself is not fully understood.”

Getting neural networks to explain how they analyse images is the focus of his current research — and of several other computer science departments and companies working on artificial intelligence.

If researchers can understand how neural networks make decisions — through visual cues or of if they could identify examples that show why their algorithms chose a particular prediction — then it will be easier to improve their accuracy and spot biases.

Even so, there are likely to be limits to their development. Neural networks need high quality data sources to train on, which simulate real world examples, but procuring such data can often be difficult. They can also be tricked by small differences between photos, intentionally made to deceive models, known as “adversarial examples”.

“I can see ways to improve the performance [of visual imaging and facial recognition neural networks],” says Mr Wang. “But I don’t see ways to get to 100 per cent.” It could be some time, researchers say, before neural networks can be reliably used for facial recognition in more security critical fields.

“I wouldn’t use them to control nuclear missiles,” says Prof Vedaldi. “But they don’t need to [reach Crime Scene Investigation levels] to be useful. They just need to be able to do something systematically on a large scale to look at the faces of thousands of people — and all of a sudden you have deployed the awesome power of a human brain and multiplied that by one thousand.”

[Copyright](#) The Financial Times Limited 2018. All rights reserved.