Time to face decisions

Civil liberty groups are raising the alarm over the ubiquitous use of automated facial recognition. As a society, we need to decide on the acceptable use of this technology and how to build in safeguards to protect human rights.

Pursued as a scientific challenge, facial recognition is an exciting direction for AI research. It pushes the limits of AI capabilities and brings to the forefront fundamental questions about the difference between artificial and human cognitive capabilities: we have a talent for recognizing faces, from any angle and in varying lighting conditions, and for accurately reading facial expressions. On the other hand, the development of facial recognition technology ticks many boxes when it comes to ethical concerns about the fast pace of innovation in AI combined with the lack of regulation and oversight. The usual risks associated with AI technology — privacy invasion, amplification of racial bias, uncontrolled power of big technology companies, malicious use — all leap to mind when considering automated facial recognition and its worrying societal implications.

However, widespread adoption is well underway and there needs to be an urgent discussion at the society level on how we want this technology to be used by private industries and the government. Facial recognition technology is already used in a range of applications, some more visible than others. Examples exist in smartphone security features, at border control for speedy passport checking, as a convenient payment method and for social robot interactions. In addition, automated facial recognition is being deployed for live mass surveillance, where images are scanned in real time and compared against databases. This is happening not only in China and the USA, but also in the UK where several police forces have had the technology since 2016 in a long-running trial. However, there is no regulation in the UK about using biometric data, other than DNA and fingerprints, and even then only police use is regulated. Biometric data such as facial features, voice, emotions and gait are not protected by law.

Credit: Simon Turner/Alamy Stock Photo

So far, the companies developing facial recognition technology are making moral judgments about whether their products are safe to use in specific applications. Shaun Moore, CEO of face recognition company Trueface, admitted in a panel discussion at CogX, a large AI conference that recently took place in London, that he has said no to potential customers "for various reasons and from different regions", following moral and ethical sales standards they developed in 2017. Microsoft has also turned down requests, such as from law enforcement in California to use facial recognition technology in police body cameras. But should such decisions be left to technology companies and their ethics boards? Indeed, Brad Smith, the president of Microsoft, last year called for the government to develop legislation in the area of facial recognition technology, pointing to the possible dangers.

The dangers have been frequently raised by civil liberty groups, particularly regarding ubiquitous automated facial recognition in everyday life at work, school or public spaces. These practices seem to be a violation of the right to privacy, one of the fundamental human rights: a principle that is currently being put to the test in a case brought to court by a civilian who accuses the South Wales police force of unlawfully using face recognition technology on him in a public space.

A common response to these worries is that if you have nothing to hide, you have nothing to fear, and that using this technology for policing could be highly effective in locating persons of interests. However, our faces are integral to our identities, and our democratic freedoms of expression and assembly won't remain the same if we are continuously tracked this way. Furthermore, a deep concern about using facial recognition in live surveillance is that — by its very design — minorities and the disadvantaged will suffer the most from its widespread use. Indeed, it is well known that facial recognition has high error rates for women and people of colour. Even if such classification biases are removed by further technological improvements, existing injustices are likely to be amplified by applications of this technology.

We need to decide when it is acceptable to gather, process and store personal biometric information, and when AI technologies like facial recognition that exploit this data are safe and acceptable to use. These decisions shouldn't be left to technology companies, which have so far competitively pursued AI technologies with little regard for human privacy. ❐

Published online: 9 July 2019
https://doi.org/10.1038/s42256-019-0074-8