Big Brother facial recognition needs ethical regulations

July 23 2018, by William Michael Carter

Credit: cottonbro studio from Pexels

My mother always said I had a face for radio. Thank God, as radio may be the last place in this technology-enhanced world where your face won't determine your social status or potential to commit a crime.

RealNetworks, the global leader of a technology that enables the seamless digital delivery of audio and video files across the internet, has just released its latest computer vision: A machine learning software package. The hope is that this new software will detect, and potentially predict, suspicious behaviour through facial recognition.

Called SAFR (Secure, Accurate Facial Recognition), the toolset has been marketed as a cost-effective way to smoothly blend into existing CCTV video monitoring systems. It will be able to "detect and match millions of faces in real time," specifically within school environments.

Ostensibly, RealNetworks sees its technology as something that can make the world safer. The catchy branding, however, masks the real ethical issues surrounding the deployment of facial detection systems. Some of those issues include questions about the inherent biases embedded within the code and, ultimately, how that captured data is used.

The Chinese model

Big Brother is watching. No other country in the world has more video surveillance than China. With 170 million CCTV cameras and some 400 million new ones being installed, it is a country that has adopted and deployed facial recognition in an Orwellian fashion.

In the near future, its citizens, and those of us who travel there, will be exposed to a vast and integrated network of facial recognition systems monitoring everything from the use of public transportation, to speeding to how much toilet paper one uses in the public toilet.

The most disturbing element so far is the recent introduction of facial recognition to monitor school children's behaviour within Chinese public schools.

As part of China's full integration of their equally Orwellian social credit system —an incentive program that rewards each citizen's commitment to the state's dictated morals—this fully integrated digital system will automatically identify a person. It can then determine one's ability to progress in society—and by extension that person's immediate family's economic and social status —by monitoring the state's non-sanctioned behaviour.

In essence, facial recognition is making it impossible for those exposed to have the luxury of having a bad day.

Facial recognition systems now being deployed within Chinese schools are monitoring everything from classroom attendance to whether a child is daydreaming or paying attention. It is a full-on monitoring system that determines, to a large extent, a child's future without considering that some qualities, such as abstract thought, can't be easily detected or at best, looked upon favourably, with facial recognition.

It also raises some very uncomfortable notions of ethics or the lack thereof, especially towards more vulnerable members of society.

Need for public regulation

RealNetworks launch of SAFR comes hot on the heels of Microsoft president Brad Smith's impassioned manifesto on the need for public regulation and corporate responsibility in the development and deployment of facial recognition technology.

Smith rightly pointed out that facial recognition tools are still somewhat skewed and have "greater error rates for women and people of colour." This problem is twofold, with an acknowledgement that the people who code may unconsciously embed cultural biases.

The data sets currently available may lack the objective robustness required to ensure that people's faces aren't being misidentified, or even worse, predetermined through encoded bias as is now beginning to happen in the Chinese school system.

In an effort to address this and myriad other related issues, Microsoft established an AI and Ethics in Engineering and Research (AETHER) Committee. This committee is also set up to help them comply with the European Union's newly enforced General Data Protection Regulation (GDPR) and its eventual future adoption, in some form, in North America.

Smith's ardent appeal rightly queries the current and future intended use and deployment of facial recognition systems, yet fails to address how Microsoft or, by extension, other AI technology leaders, can eliminate biases within their base code or data sets from the onset.

Minority report

The features of our face are hardly more than gestures which force of habit has made permanent.—Marcel Proust, 1919

Like many technologies, Pandora has already left the box. If you own a smart phone and use the internet, you have already opted out of any basic notions of personal anonymity within Western society.

With GDPR now fully engaged in Europe, visiting a website now requires you to "opt in" to the possibility that that website might be collecting personal data. Facial recognition systems have no means of following GDPR rules, so as such, we as society are automatically "opted-in" and thus completely at the mercy of how our faces are being recorded, processed and stored by governmental, corporate or even privately deployed CCTV systems.

Facial recognition trials held in England by the London Metropolitan Police have consistently yielded a 98 per cent failure rate. Similarly, in South West Wales, tests have done only slightly better with less than 10 per cent success.

Conversely, University of California, Berkeley, scientists have concluded that substantive facial variation is an evolutionary trait unique to humans. So where is the disconnect?

If as Marcel Proust has suggested, our lives and thus our personalities are uniquely identifiable by our faces, why can't facial recognition systems not easily return positive results?

The answer goes back to how computer programming is written and the data sets used by that code to return a positive match. Inevitably, code is written to support an idealized notion of facial type.

As such, outlying variations like naturally occurring facial deformities or facial features affected by physical or mental trauma represent only a small fraction of the infinite possible facial variations in the world. The data sets assume we are homogeneous doppelgängers of each other, without addressing the micro-variations of peoples faces.

If that's the case, we are all subject to the possibility that our faces as interpreted by the ever-increasing deployment of immature facial recognition systems will betray the reality of who we are.

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

Provided by The Conversation