NUS National University of Singapore

Source: *The Straits Times*, pA26
Date: 7 December 2019

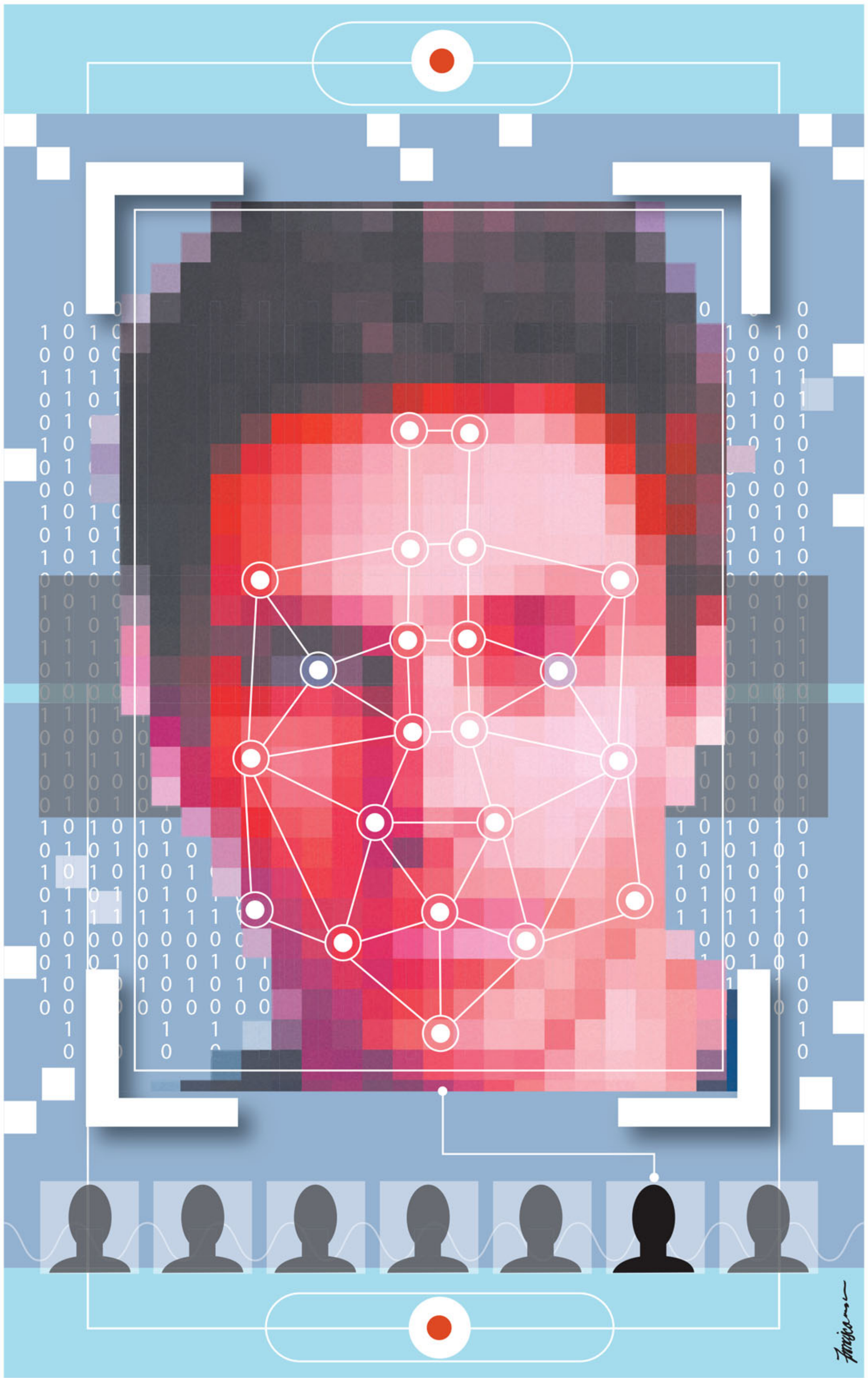
ByInvitation

Facing up to facial recognition technology

The benefits of facial recognition technology are that it offers a quick, non-invasive means of identifying people. Those are also its dangers.

Simon Chesterman

For The Straits Times



As facial recognition technology continues to improve, one day we may not need to remember faces – much as few of us now bother to memorise telephone numbers. But those faces would not be forgotten. They would be digitised and stored. The question is how that data will be used, by whom, and in what circumstances.

Last month, it was reported that facial recognition will be used to take attendance in Singapore's Parliament and check into certain hotels. The latest phones already unlock with Face ID and many buildings – including University Hall at the National University of Singapore – use face scans to control entry.

This use of biometrics for security – relying on the uniqueness of your face, fingerprint or iris – offers the prospect of a world without passwords to remember or identity cards to show. Facial recognition in particular is fast, contactless and able to identify multiple people at the same time. These benefits could smooth movement through passport control or keep a vigilant eye out for known criminals. Yet those same qualities could also enable mass surveillance on an unprecedented scale.

Silicon Valley has been at the forefront of many advances in facial recognition technology. Yet it is striking that San Francisco, a mere half-hour drive away, was the first city in the US to ban its use.

It is not too late to impose limits on how facial recognition is used. Unfortunately, it may also be too early.

DON'T SMILE

Facial recognition, a subset of image recognition, is a field that has advanced swiftly in the past few years with the help of artificial intelligence (AI). Early systems required that subjects remain still with a neutral expression. Today, Face ID works from multiple angles in low-lighting, and can even distinguish between "identical" twins.

Training such systems to improve the quality of outcomes requires a large database of images. That's why leaders in the field include Apple and Facebook, whose users upload vast numbers of images – helpfully tagging or correcting tags, improving the algorithms at no cost to the companies themselves.

A particular challenge is that, unlike Dorian Gray, our faces change as we age. Cue Instagram's 10-Year Challenge, which was a fun meme earlier this year that showed who has aged well or not – and, perhaps, harvested additional training data for algorithms to adapt to the wrinkles and lines that will develop on its archive of images.

Facial recognition is now used for border security in Australia, Canada and the US, as well as entry control for a growing number of buildings around the world. Its proposed use in Singapore's Parliament points to a wider range of uses, however. Instead of confirming the identity of one person, it could be used to monitor the movements of many.

BIG BROTHER, WHERE ART THOU?

China is often presented as the bugbear in this scenario. Despite breathless commentary about its social credit system, the Chinese Communist Party is not able to track the movements of 1.3 billion people in real time. Yet.

The technology has been deployed in Xinjiang as part of a range of efforts to monitor and control the Uighur population. One of the reasons why masks have been such a point of controversy in the ongoing protests in Hong Kong is the chilling effect of the authorities being able to identify even peaceful protesters.

With an estimated 170 million cameras across China, the images captured support the surveillance activities of the government but also provide data for China's AI sector.

Yet people in many countries are now acclimated to widespread use of surveillance cameras in public spaces. London remains at the forefront of Western democracies, with more than 500,000 cameras or one for every 15 persons. (The same study by Comparitech estimated that Singapore has about 86,000 cameras, or one for every 65 persons). Even if we might bristle at stationary cameras, virtually every passer-by also has a high-definition camera in his or her pocket or purse.

Similarly, most of us seem nonchalant about facial recognition, allowing ourselves to be tagged in photos automatically or by "friends" on social media.

Putting these two things together, however, should give most readers pause. It is one thing to have your identity verified when unlocking your phone, entering the country, or voting in Parliament. It is quite another to be identified and logged every time you step onto the street, ride in a taxi or enter a shop.

You probably would not want to have to show ID in such situations. Indeed, last September new rules limited the manner in which organisations can collect NRIC and other national identification numbers in Singapore. Given that it is harder to change your face than to change your NRIC, it may be time to develop similar guidelines on the use of facial recognition.

Unfortunately, that's easier said than done.

THE REGULATION DILEMMA

Writing in 1980, Dr David Collingridge, a professor in Birmingham, observed that any effort to control new technology faces a double bind. During the early stages, when control would be possible, not enough is known about the technology's harmful social consequences to warrant slowing its development. By the time those consequences are apparent, however, control has become costly and difficult.

The climate emergency offers an example. Before automobiles entered into widespread usage, a 1906 Royal Commission studied the potential risks of the new machines plying Britain's roads. Chief among those was thought to be the dust that such vehicles threw up behind them.

A century later, better roads and mud flaps have taken care of the dust situation. Meanwhile, transport contributes about a quarter of the world's carbon dioxide emissions with few signs of slowing down.

Social media offers another. In retrospect, regarding elaborate software platforms like Facebook and Twitter as "free" was always naive. But data protection laws were in their infancy as users' personal data was monetised and weaponised. It is probably too late now to reverse the economic model of the World Wide Web – although one of its original architects, Mr Tim Berners-Lee, at least wants to try.

In the case of facial surveillance, it is not yet too late.

But is it too early?

The warning signs are apparent and some preemptive lawsuits have been launched – with recent victories in Sweden, where a secondary school was fined for using facial recognition to track attendance, and England, where its use at a development in King's Cross was scrapped after a backlash.

In the US, the American Civil Liberties Union is asking a federal court to demand that the Federal Bureau of Investigation and other agencies reveal their own use of the technology. There is also a movement to distinguish clearly between facial identification and facial surveillance.

In the Singapore context, the new rules on NRIC numbers offer a starting point. Organisations can only collect such details when it is necessary to verify an individual "to a high degree of fidelity". The same principles could apply to biometric data.

As for the Government, the commitment to transparency and accountability in the handling of data following last week's Public Sector Data Security Review Committee report should help build trust in how such personal data is safeguarded. (Disclosure: I was a member of the committee's Expert Group).

AS PLAIN AS THE NOSE ON YOUR...

"I never forget a face," Groucho Marx famously quipped. "But in your case I'd be glad to make an exception."

As facial recognition technology continues to improve, one day we may not need to remember faces – much as few of us now bother to memorise telephone numbers.

But those faces would not be forgotten. They would be digitised and stored. The question is how that data will be used, by whom, and in what circumstances.

This is not the end of the battle over facial recognition. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.

stopinion@sph.com.sg

• Simon Chesterman is dean and professor of the National University of Singapore Faculty of Law, which this week launched a new Centre for Technology, Robotics, AI & the Law.