BUDDLE FINDLAY

Facing the facts: Privacy issues with facial recognition technology

Allan Yeoman

6 December 2019

Facial recognition technology has quietly integrated into a number of areas of everyday life. In addition to the more obvious security, public safety and surveillance applications (which have led, for example, to Hong Kong protesters wearing masks and felling lampposts equipped with facial recognition CCTV cameras in order to avoid identification), the technology is increasingly being used as a retail tool to track customer behaviours and movement to generate predictive consumer analytics. And New Zealand is following suit. Last year the NZ Herald reported on a major supermarket chain having deployed facial recognition CCTVs in some of its stores and more recently on two tertiary institutions trialling the technology to monitor student attendances in New Zealand. But how does this increasingly common technology fit within global trends towards greater privacy, control and transparency over data collection and use?
There are three key privacy issues that tend to arise in facial recognition privacy discussions:

First, facial recognition software can only work alongside a rich database of facial images, so the recognition algorithm can be trained to detect faces, and to then match a detected face to an identity in the database. Populating and using facial image databases raises all sorts of questions regarding the source of those images, the extent of any consent or authorisation obtained, the potential uses to which the images will be put and how they will be protected through storage and security. There have been reports that some facial recognition software products already in use have been trained on images of individuals mined from the internet and obtained without consent. In the absence of appropriate consents, these products may simply breach the law.

Second, independent tests of facial recognition technology have repeatedly shown that it is far from perfect or reliable, presenting a meaningful challenge to compliance with Information Privacy Principle 8 under New Zealand's (current) Privacy Act and equivalent legislation around the world. Principle 8 requires that "An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading." If an agency was collecting images and using unreliable technology to match that image to an individual it is difficult to see how it could comply with this principle. Facial recognition technology relies heavily on the quantity and quality of the data fed into it. The potential for misidentification and error rates due to gender and racial biases in algorithms are known to be high, even with the best software of its kind, with disproportionately higher error rates among certain ethnic and racial groups. Depending on the function, flaws in facial recognition software could have catastrophic impacts.

Third, and as is often the case with applying legal frameworks of any type (not just privacy) to fast-moving technological developments, the law has not always kept up with the pace of change which leads to varying approaches taken by courts and privacy regulators around the world. This means that it can be difficult to identify in practice what uses of facial recognition technology will breach the law. For example, while the legality of the use of facial recognition technology by South Wales police was recently tested and found by the High Court in Cardiff not to breach the law, in San Francisco, city authorities have simply banned its use by the police and government agencies for now on the basis that there is insufficient legal or regulatory framework to deal with the issue.

In New Zealand, the Office of Privacy Commissioner (OPC) has, however, provided some guidance. The OPC has advised agencies that the use of facial recognition technology should be subject to a high level of scrutiny over its accuracy and whether it has been thoroughly tested for use in New Zealand. The OPC recommends that an agency contemplating deploying this kind of technology undertake a Privacy Impact Assessment before doing so, and warns of the grave ramifications of getting it wrong (for example, mistakenly branding someone a shoplifter). In light of that guidance, organisations in New Zealand looking to implement facial recognition technology – in any context – would be wise to proceed with a high degree of care, particularly given the greater fines and scrutiny that will come into force under the new Privacy Bill in 2020.

This article was written by Allan Yeoman and Jennifer Yang for the NBR (December 2019).

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659