Your face is part of Australia's 'national security weapon'—should you be concerned?

September 14 2015, by Adam Molnar

Images of your face can be checked against images held on government databases. Credit: Flickr/StephenMitchell , CC BY-NC-ND

Australian government plans to increase the use of facial recognition in its counter-terrorism strategy raise concerns about privacy and how the technology will be used in everyday policing.

Details of the A$18.5 million National Facial Biometric Matching Capability were announced last week by Michael Keenan, the minister for justice and the minister assisting the prime minister on counter-terrorism.

Keenan said the scheme – known as "the capability" – will allow Commonwealth agencies and state law enforcement to try to match a photograph of an unknown person with photographs on government records, such as passports and driving licences. The aim is to help put "a name to the face of terror suspects, murderers and armed robbers" and other criminals.

This comes on the heels of government amendments to the Migration Amendment (Strengthening Biometrics Integrity) Bill 2015 in late August. These laws introduced a broad discretionary power for several Australian agencies to collect biometric data on both Australian citizens and non-citizens at the border and within Australia.

These amendments are expected to add even more records to the more than 100 million facial images already held by agencies that feed into the capability.

Privacy concerns

A closer examination of the capability reveals a number of concerns about its expected effectiveness and its impact on privacy.

If your passport, credit card, PIN or tax file number are compromised due to a security breach, they can be replaced fairly easily. Not so with your facial features. If a biometric database is hacked, the information can potentially be abused by criminals over your entire life.

The government insists the capability entails "strong privacy safeguards"

but does not provide much detail beyond noting that facial recognition records will not be stored in a centralised database.

Instead, the records will be held by participating agencies, which will be able to reach in to one another's records. But will it be effective? And what are the risks for privacy and human rights?

False positives

Biometrics and facial recognition are big business these days, but are still not foolproof. Credit: NEC Corporation of America, CC BY

Current research shows that the latest facial technology is still plagued with error rates and inaccuracies.

Images collected through CCTV or social media platforms are hampered by poor lighting or indirect angles of faces, so it is often difficult to find an accurate match. For example, even with the volume of footage of the Boston Marathon bombing suspects, facial recognition wasn't enough to identify the assailants.

It is also unclear how much the use of facial recognition is actually helping police make arrests.

There is also the question of accuracy. The FBI reportedly has a 20% error rate for its Next Generation Identification program.

In Australia there is no clear indication what authorities are willing to accept as an error rate when using facial recognition technology.

Like the data retention amendments, regulation of the collection and sharing of biometric identifiers in Australia is subject to executive ministerial discretion. Any other regulation of the capability is left to weak privacy legislation (which many of the agencies involved in the capability are exempt from) in the absence of a formal bill of rights.

From overseas wars to domestic policing

Facial recognition has been a part of military and intelligence operations in overseas conflicts in Afghanistan and Iraq.

Now the technology will find its way into routine policing environments in Australia, aided by mobile hand-held devices such as tablets, smartphones and even wearable cameras.

In a policing context, this raises new questions that push the legal envelope on the collection of biometric identifiers without meaningful consent when using mobile devices in the field.

The use of facial recognition identification in policing introduces the possibility that law enforcement might want to stop an individual simply to check, and potentially collect, their facial recognition print. They could also use the technology to identify people at a political protest or major sporting or music event.

Jennifer Lynch, a senior staff attorney with the civil liberties advocacy group Electronic Frontier Foundation, notes that the use of facial recognition technologies in routine policing "pushes the line of what's legal".

Security risks

The Australian government is seeking to quell any concerns about privacy over the mass biometric archive by insisting that the capability will not be a centralised database.

But an integrated network of shared records is actually even more vulnerable to penetration simply because the prospective attack surface is larger.

The only way to actually ensure privacy is to limit initial collection and restrict the use of any biometric records. If they are to be used at all, it should be for only very specific purposes.

Given that there is no clear evidence on the expected effectiveness of the capability, which has already spread into a whole-of-government initiative, critical questions remain about the risks posed by Australia's newest mass surveillance weapon.

Source: The Conversation