THE CONVERSATION

Academic rigour, journalistic flair

Many more faces to be added to a national database, but will it make us any safer? Shutterstock copy/Andrey_Popov

Let's face it, we'll be no safer with a national facial recognition database

October 6, 2017 1.49pm AEDT

Author

Bruce Baer Arnold

Assistant Professor, School of Law, University of Canberra

A commitment to share the biometric data of most Australians – including your driving licence photo – agreed at Thursday's Council of Australian Governments (COAG) meeting will result in a further erosion of our privacy.

That sharing is not necessary. It will be costly. But will it save us from terrorism? Not all, although it will give people a false sense of comfort.

Importantly, it will allow politicians and officials to show that they are doing something, in a climate where a hunt for headlines demands the appearance of action.

Read more:* *Leaders agree to hand over driver licence data as part of COAG counter-terror package

Your biometric data

Biometric data used in fingerprint and facial recognition systems is indelible. It can be used in authoritative identity registers, featured on identity documents such as passports and driver licences.

It can be automatically matched with data collected from devices located in airports, bus and train stations, retail malls, court buildings, prisons, sports facilities and anywhere else we could park a networked camera.

Australia's state and territory governments have built large biometric databases through registration of people as drivers – every licence has a photograph of the driver. The national government has built large databases through registration for passports, aviation/maritime security and other purposes.

Irrespective of your consent to uses beyond those for which the picture was taken, the governments now have a biometric image of most Australians, and the ability to search the images.

COAG announced that the governments will share that data in the name of security.

Sharing data with who?

Details of the sharing are very unclear. This means we cannot evaluate indications that images will be captured in both public and private places. For example, in retail malls and libraries or art galleries – soft targets for terrorism – rather than in streets and secure buildings such as Parliament House.

Prime Minister Malcolm Turnbull has responded to initial criticism by clarifying that matching will not involve "live" CCTV.

But the history of Australian surveillance law has been a matter of creep, with step-by-step expansion of what might initially have been an innocuous development. When will law enforcement agencies persuade their ministers to include live public or private CCTV for image matching?

We cannot tell which officials will be accessing the data and what safeguards will be established to prevent misuse. Uncertainty about safeguards is worrying, given the history of police and other officials inappropriately accessing law enforcement databases on behalf of criminals or to stalk a former partner.

The sharing occurs in a nation where Commonwealth, state and territory privacy law is inconsistent. That law is weakly enforced, in part because watchdogs such as the Office of the Australian Information Commissioner (OAIC) are under-resourced, threatened with closure or have clashed with senior politicians.

Australia does not have a coherent enforceable right to privacy. Instead we have a threadbare patchwork of law (including an absence of a discrete privacy statute in several jurisdictions).

The new arrangement has been foreshadowed by governments over several years. It can be expected to creep, further eroding privacy and treating all citizens as suspects.

Software and hardware providers will be delighted: there's money to be made by catering to our fears. But we should be asking some hard questions about the regime and questioning COAG's statement.

Let's avoid a privacy car crash

Will sharing and expansion of the biometric network – a camera near every important building, many cameras on every important road – save us from terrorism? The answer is a resounding no. Biometrics, for example, seems unlikely to have saved people from the Las Vegas shooter.

Will sharing be cost effective? None of the governments have a great track record with major systems integration. The landscape is littered with projects that went over budget, didn't arrive on time or were quietly killed off.

Think the recent Census and Centrelink problems, and the billion dollar bust up known as the Personally Controlled Electronic Health Record.

It won't be improved by a new national ID card to fix the Medicare problem.

Is the sharing proportionate? One answer is to look at experience in India, where the Supreme Court has comprehensively damned that nation's ambitious Aadhaar biometric scheme that was meant to solve security, welfare and other problems.

The Court – consistent with decisions in other parts of the world – condemned the scheme as grossly disproportionate: a disregard of privacy and of the dignity of every citizen.

Read more: COAG meeting on counter-terrorism was more about politics than practice

---

Is sharing likely to result in harms, particularly as the biometric network grows and grows? The answer again is yes. One harm, disregarded by our opportunistic politicians, is that all Australians and all visitors will be regarded as suspects.

Much of the data for matching will be muddy – some street cameras, for example, are fine resting places for pigeons – and of little value.

As with the mandatory metadata retention scheme, the more data (and more cameras) we have the bigger trove of indelible information for hackers. Do not expect the OAIC or weak state privacy watchdogs (which in some jurisdictions do not exist) to come to the rescue.

As a society we should demand meaningful consultation about official schemes that erode our rights. We should engage in critical thinking rather than relying on headlines that reflect political opportunism and institutional self-interest.

The incoherent explanation and clarifications should concern everyone, irrespective of whether they have chosen to be on Facebook – and even if they have nothing to hide and will never be mistaken for

someone else.

Privacy Surveillance COAG Facial recognition Biometrics CCTV Data privacy Identity card