Close up: the government’s facial recognition plan could reveal more than just your identity

A Bill to set up the federal government’s biometric identity system is currently going through Parliament. But there are concerns over just how much information the system would be allowed to gather, and how that might be used to establish more than just the identity of a person.

Strongly based on the FBI model in the United States, the Identity Matching Services Bill and its Explanatory Memoranda prescribe what data can be collected, shared and processed, by who and for what purposes.

Read more: Let’s face it, we’ll be no safer with a national facial recognition database

The Bill is based on the Council of Australian Governments (COAG) agreement, signed in October 2017.

The public purpose of the system is to provide identity-matching services to government agencies and some private entities (such as banks and telcos). But the Bill will also establish the Department of Home Affairs as an incredibly data-rich law-enforcement and security agency, with a wide remit for data collection and use.

Accessing the ‘hub’

The first layer of the identity matching system is what’s called the “interoperability hub”. This is the interface for those government and private entities seeking access to identity services.

These identity services effectively answer the questions: “is this person who they say they are?” and “who is this person?”.

The hub works on a query and response model. This means that users of the system do not have access to any of the underlying data powering the biometric processing. They won’t be able to browse the databases; they will only have their identity verification questions answered.

The second layer of the system, underneath the hub, is the databases that drive the biometric identity matching. These include passport and citizenship information as well as the new National Drivers License Facial Recognition Solution database, which will be housed in the Department of Home Affairs.
Along with images, these databases include an extraordinary amount of personal information. Roads agencies, like VicRoads in Victoria, hold rich databases of biographical information including names and addresses, age and gender. Those records are also linked to information about vehicle ownership and registration.

Commonwealth criminal intelligence agencies have been seeking access to state-held driver’s licence images and associated personal information for years. The 2017 COAG agreement is what will finally enable a Commonwealth agency to have custodianship over this data on behalf of states.

You ask, it collects

But the use of the hub for identity-matching services means that the amount of data in these database will grow. Each time a user makes a request for identity-matching services, the hub will supply more data to the Department.

The Department can collect and process all information included in an identity document that has a photograph. It can also collect all of the information associated with that document held by the authority that created it.

When an entity (like law enforcement) seeks identity verification, it will likely supply images from its own camera or CCTV systems (or supplied by other parties), along with whatever data associated with those images that might help identify the person.

That could include where and when the images were taken or supplied, and potentially what a person was doing at the time the image was taken or supplied. All of those data are provided to the Department of Home Affairs when an identity verification is done.

Similarly, when banks and telecommunications companies use the hub, that potentially links those records to the Department databases - or at least facilitates those linkages down the track.

This creates the possibility of aggregated criminal and civil histories in a single identity record, like what has occurred with the FBI’s biometric system in the US.

This is all without access to the largest, most sophisticated facial recognition database in existence: Facebook. If sources such as public CCTV and social media are eventually linked into the system, its significance changes again, radically.

Joining the dots

So what is all this data for? On one hand, it provides identity services to hub users. But on the other hand, it generates insights on behalf of the Department of Home Affairs for the sake of policing. Data at a large scale, and especially when used in the context of security and intelligence, means insights and predictions.

The purposes for which the Department can use the information it gathers are very broad. They include preventing and detecting identity fraud, law enforcement, national security, protective security (protection of government assets, persons or facilities), community
safety (for instance where a person is acting suspiciously in a crowded public place), and road safety.

Those categories include criminal intelligence gathering and profiling, policing of public spaces and public events, and policing of activist communities and protests.

Many of these policing exercises are highly data-driven, using new predictive techniques to identify criminal suspects and political agitators before any activity has even occurred.

Identity technologies have historically been used by governments to answer two questions: 1) What person is that? 2) What kind of person is that?

Identity is more than merely biographical information. It is a narrative that we tell about ourselves and that others tell about us. That narrative is what is at stake in this type of security surveillance.

Beyond facial recognition, we have already seen machine vision systems designed to predict sexuality on the basis of a person’s image. It’s research that has already generated plenty of controversy.

Read more: Machine gaydar: AI is reinforcing stereotypes that liberal societies are trying to get rid of

If the data sets can be construed, and the results are to be accepted, there is no reason why machine vision systems cannot be targeted to answer questions about criminal propensity, IQ, suitability for certain tasks, political leanings, or anything else.

We need to understand what these new database arrangements will enable in terms of high-level or political policing by the Department of Home Affairs, and what this new technical and bureaucratic architecture means for Australia’s broader surveillance arrangements.