THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

Centre for Policy Futures

24 September 2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Email: pjcis@aph.gov.au

Dear Committee Chair

Re: *Identity-matching Services Bill 2018* in relation to face-matching services

Thank you for the opportunity to submit a late submission to your review into the *Identity-matching Services Bill 2018*, in which it is proposed that a new facility for cross jurisdictional face-matching services will be made operable.

I am writing to express my concern that the proposed system design of the face-matching service is problematic and falls well short of best practice for data protection and privacy principles. Alternative designs are possible that better meet the 'privacy by design' approach that is regarded as an industry standard. I would urge the Committee to recommend the Government revisit its system design in order to better enhance citizen data protection and privacy as well as reduce the possibility of cybercrime.

In what follows I outline the face-matching system design proposed by the Government, the problems with such an approach, and outline an alternative design. I also attach a piece I authored on *The Conversation* about this issue (with online comments), as well as government responses to my previous correspondence highlighting the problems with the Government's proposed approach.

The proposed system design of the face-matching service

The Government has proposed the creation of an additional central database of personal information from State and Territory driver's license databases. This database would contain the photo image of a person and other personal information, such as name, date of birth and address, as recorded in the State and Territory driver's license systems. In short, the proposed new database would replicate all the State and Territory driver's license databases into one large database; that is, an amalgamated copy. A key distinction is that the central database will be segmented along jurisdictional lines. "Driver licence images will be made available via a common facial recognition system, hosted by the Commonwealth on behalf of participating state and territory driver licencing agencies." (https://www.homeaffairs.gov.au/crime/Documents/face-matching-services-fact-sheet.pdf). This is to ensure that data collected in each state and territory is only accessible to people within that jurisdiction, which accords to the privacy and data protection principle of disallowing sharing of data for purposes not associated with the reasons it was collected.

This new central database will sit alongside similar databases already owned and operated by the Commonwealth that contain visual images of people (i.e. passports, VISA and citizenship data).

The way the Face Verification Service (FVS) and Face Identification Service (FIS) work is through a central hub. An authorised user will be able to post a photographic image to that hub, which will then search all the central databases for a match. In the FVS, in addition to an image, a user will need to provide the service with the person's name and other information (such as date of birth), and the Service will respond whether the information the user has matches a person's visual and personal data within any of the connected databases or not; a yes/no response. In the FIS, a user will be able to submit a photograph and request the personal information matching that image if it is stored in any of the connected databases.

Problems with the proposed design

It is my assessment that the proposed centralised database ***is*** consistent with current data protection and privacy laws. However, the risks to data protection and privacy breaches could be importantly reduced with a different design.

The key problem with the proposed design is that is involves an unnecessary replication of databases from each state and territory in a segmented centralised database. This consequently means that each data update at the state/territory level systems – such as changes of address, new photographs, new license holders – needs to be correspondingly updated in the central database. It is not clear how this updating process will occur (for example, immediately via live updating, or in overnight batched processes). This updating process adds data protection risk to the overall design, because such data transfers can be intersected. Unless the data is immediately updated through a constant online connection, this design also reduces a delay in the accuracy of data in the central system.

A further problem with a centralised database is that it becomes a more attractive honeypot for hackers than eight separate databases.

Finally, there is the potential of mission creep that the centralised database facilitates. With proposals for increased data sharing that circumvents privacy laws as part of the new National Office of Intelligence (e.g. thesaturdaypaper.com.au/news/law-crime/2018/09/22/new-domestic-intelligence-powers/15375384006887), a centralised database provides little protection for privacy and constraint to authorities to ensure due process is followed.

An alternative system design for a face-matching service

The good news is that there is an alternative to the proposed centralised database that provides all of the functionality that the government is seeking as well as stronger data security and privacy protections through technical measures.

Instead of the proposed central Hub providing a query to the centralised databases for driver's licences, passports, and VISA/citizenship, the Hub could instead query each of the 8 state and territory driver's licenses databases.

This means that data traffic between state/territory databases is much smaller (and thus less prone to intersection) and that the data traffic is limited to only queries about facial recognition, rather than updates of all licensed drivers in Australia.

Objections from the Commonwealth Attorney-General to my suggested approach were outlined in a letter dated 23 November 2017 (see attached):

> *A centralised model is also expected to deliver better performance than the majority of the alternatives. Speed of insight is paramount in a system intended to provide national security, law enforcement and community safety benefits, and potential delays caused by bandwidth 'chokepoints' between any of the major centers would be untenable.*
>
> *Providing each State and Territory road agency with its own facial matching engine was not considered to be as cost-effective as a centralised solution, and could potentially raise interoperability issues with those jurisdictions that already utilise facial recognition technology.*

A key argument is speed. Whilst speed may well be important in some cases, highly time-critical responses are not among the reasons for a facial matching service by the Department of Home Affairs (https://www.homeaffairs.gov.au/crime/Documents/face-matching-services-fact-sheet.pdf). Moreover, the differences in time searching a centralised database compared to parallel searches of 8 state/territory databases is arguably so miniscule to not be mentionable. Indeed, information scientists understand that parallel searches in 8 separate databases is technically faster than that of one large centralised database. In short, this argument appears to be an excuse, rather than based on technical capacity.

The second argument above relating to interoperability and cost effectiveness also does not hold under close scrutiny. Interoperability is also needed to create a centralised database, as proposed. Moreover, greater investment in interoperability of compatible facial matching engines in state and territory databases could arguably have longer term benefits for collaboration between jurisdictions.

My expertise

I make this submission based on my expertise in technology and public regulation. I hold a first class honours degree in computer science, and have over 20 years' experience in researching the use of digital technologies by government around the world. I have led several international studies, variously funded by the Australia Research Council, and IBM. As an example of my prescient work, 15 years ago my research highlighted the challenges of algorithmic profiling and targeting, that is now only getting attention in the post Cambridge Analytica world. I am currently a Principal Research Fellow at the University of Queensland's Centre for Policy Futures, and leading a multiyear collaboration with CSIRO to examine the governance and regulatory challenges of new technologies. I am not a lawyer and have not sought to assess the legal framework being proposed. More information about my expertise can be found at http://researchers.uq.edu.au/researcher/708.

I would be pleased to provide any further input into your Committee should that be helpful.

Yours sincerely

[redacted]

Dr Paul Henman, BScHons (computer science), PhD, GCEd
Principal Research Fellow, Centre for Policy Futures &
Associate Professor of Digital Sociology and Social Policy, School of Social Science
University of Queensland
[redacted]