PJCIS Inquiry

Identity-Matching Services Bill 2018

and

The Australian Passports Amendment (Identity-Matching Services) Bill 2018

Supplementary Submission

A joint submission from:
NSW Council for Civil Liberties
Liberty Victoria
Queensland Council for Civil Liberties
South Australian Council for Civil Liberties
Australian Council for Civil Liberties

31/3/2018

1. The Joint CCLs made an initial submission to the PJCIS on the detail of *The Identity-matching Services Bill 2018* and *The Australian Passports Amendment (Identity-Matching Services) Bill 2018*[1] arguing for amendments which would both limit the scope of the proposals and provide stronger protections for the ever diminishing right to privacy. We are pleased to have the opportunity to make this supplementary submission on the same Bills.
2. We gave priority to making comment on the detail of the Bills because, given the agreement already reached by COAG and the enthusiastic and uncritical endorsement by state and federal government leaders of that agreement[2], it is clear that some version of this legislation is going to be passed by the Parliament. Thus our most urgent focus was on arguing for achievable amendments to lessen the potential harm from the Bills.
3. In this supplementary submission the CCLs reaffirm our deep concerns about the wisdom and long term implications of the significant expansion in the national identity matching services framework. Our view is that this further development in the capacity for national mass surveillance of the population by the state will have, over time, significant damaging implications for the nature of our society and the robustness of our democracy.
4. We noted at the time of the COAG announcement[3] that the untroubled endorsement of the package and blithe dismissal of any concerns about the impact on privacy or traditional liberties by our political leaders did not inspire confidence they would give a high priority to the promised 'robust privacy safeguards' or that they fully appreciated the risks associated with the linking of the technical identity-matching capability of the enhanced interoperability hub with a national facial

---

[1] Joint CCLs submission to the PJCIS Inquiry into The Identity-matching Services Bill 2018 and The Australian Passports Amendment (Identity-Matching Services) Bill 2018, Submission number 9, 21/3/2018 [JCCLs PJCIS submission number 9]
[2] Only the ACT Chief Minister raised concerns about privacy and civil liberties but none the less the ACT 'more in sorrow' than enthusiasm also signed up to the COAG agreement. ABC PM 5/10/2017
[3] NSWCCL Website : Civil liberties bodies reject massive facial recognition database, posted 6/10/17.http://www.nswccl.org.au/free_speech_censorship_privacy; Joint Media Release: Joint CCLs, Electronic Frontiers Australia, Australian Privacy Foundation, Digital Rights Watch:6/10/17 ; Public Statement by Liberty Victoria:*PM CALLS FOR NATIONAL DATABASE OF DRIVER'S LICENCE PHOTOS* 6/10/17.

recognition data base. (We were not wide of the mark. Our initial submission documents the failures of the Bill to deliver on promised 'robust privacy safeguards'[4].)

5. Our concern is heightened as the national facial recognition database is moving closer to encompassing the whole population – potentially incorporating all identity documents with digital facial images issued by any government agency.
6. We note the assurance in the Explanatory Memorandum that the *'interoperability hub facilitates data-sharing between agencies on a query and response basis, without storing any personal information*[5] and that passport, visa and citizenship images will continue to be held by their current agencies. The new *'federated database of identification information contained in government identification documents (initially driver licences)'*[6] will be held in Home Affairs.
7. These statements seem intended to suggest that we need not be concerned by the proposals because a single national identity database is not being created in any one physical place - and that nothing much is changing beyond enhanced speed and efficiency for law enforcement agencies.
8. The Prime Minister has also explicitly asserted that the enhanced system will not amount to 'mass surveillance' because CCTV footage - collected from thousands of public locations - would not be stored in the new database. This statement appears to have been an attempt to correct his previous description of the scheme as allowing real time surveillance of persons attending sporting and entertainment events. [7]
9. In our view these are misleading assurances.
10. We don't dispute that some of the physical databases will stay with existing agencies. However, if we understand the Bill and the Explanatory Memorandum correctly, this is inconsequential. The reality is that the technical facial matching

[4] [JCCLs PJCIS submission number 9]
[5] *The Identity-matching Services Bill 2018; Explanatory Memorandum. [IMS Bill 2018:EM)] P2*
[6] ibid
[7] ABC PM 5/10/2017

capability of the interoperability hub, combined with access to identity data for most of the population, will deliver the capacity for mass surveillance by the state of most of the population in almost any public place or activity- in (almost) real time and subsequently[8].

11. It is of central importance that the Australian people be given an accurate description of the potential scope and capability of the enhanced identity matching service. Without this transparency and clarity it is impossible to make a meaningful assessment of its necessity or proportionality - or of the potential long term impact of the service on our democratic values.
12. The CCLs agree that the power to rapidly check the identity of an unidentified person of interest in a terrorist or public safety context against a comprehensive and integrated facial recognition database of persons who are in any way associated with terrorist or serious criminal activity is justified and proportionate – and would likely be of strategic use to the police or security forces dealing with the incident.
13. The current enhancement proposal goes well beyond these reasonable circumstances: the matching database encompasses everyone for whom a government issued identified facial image is available (not just known suspects) and access is provided to a broad range of government, local government and non-government entities for a wide range of non-urgent purposes which are – in our view - already adequately catered for.

Broader impacts – public political discourse and protest

14. People attending public protests have always been subject to surveillance by the state. The broader impact of this has been dependent on the possible scale of the surveillance, clarity and accuracy of images or speech recordings and the capacity to subsequently identify and locate persons.

[8] Subsequent surveillance is increasingly possible as so much CCTV is now stored for lengthy periods by the operator of the cameras.

15. The critical and transformational factor in this scheme is the enhanced capacity for unidentified facial images to be matched quickly against a massive facial recognition database.
16. Given that it is increasingly impossible to evade CCTV cameras in public spaces or in many private places (public open spaces, hotels, clubs, casinos, churches, petrol stations, airports, railway stations, shopping centres etc) we are effectively killing anonymity.
17. While there are many legitimate reasons for some people wanting to be anonymous or use pseudonyms which will be compromised by these developments, the real issue for democracy is the chilling impact of this new surveillance capacity on the right to freedom of political discourse and the right to protest and dissent.
18. There is no shortage of well documented modern history on the longer term incompatibility of the surveillance state and democracy.
19. This proposal is not a sudden development. It is the latest iteration in the development of a national facial recognition identity framework and system which have quietly evolved over the last decade or so.

Recent historical context for privacy

20. In 1987 and in 2006 the Federal Government attempted to implement national identity schemes – most memorably, the Australia Card and then the Access Card. These aimed to provide administrative efficiency but the perceived threat of increased government monitoring and surveillance and loss of privacy and the right to anonymity generated solid resistance from civil society.
21. Neither was implemented and it was reasonable to assume that, given the strength of community opposition, future Governments would be wary of trying again.
22. The post 9/11 context understandably changed the parameters of the privacy debate. We have experienced a major - albeit incremental - transformation of government powers and public attitudes in relation to privacy.
23. Protection from Government access to private information has been whittled away by expanding the range of personal information that the state can access for non-

suspects as well as persons suspected of criminal activity, and dispensing with the need for authorising warrants in many of these contexts. The initial claim that these increased powers and loss of protections were necessary to equip Governments to protect us from terrorism and other threats to national security has been expanded to other less serious contexts and purposes.

24. Simultaneously the massive expansion of social media has encouraged people to make public huge amounts of personal information that would hitherto have been largely private to oneself and close friends/family.
25. Public concern for the right to privacy has been eroded over the years since the Australia Card was successfully resisted. This is partly because a sense of futility of ongoing opposition given the surveillance/data collection powers already in Government hands and the mega data banks of personal information in the hands of social media platforms (Google, Facebook) and the corporations who have bought this personal information to be used for commercial gain and political parties – exempted from Privacy Laws - who amass personal data from all accessible sites for political gain.
26. The recent revelations as to the massive sweeping up and apparently malevolent use of the personal information of many millions by Cambridge Analytica has clearly jolted many to reconsider their practice in relation to social media platforms such as Facebook. Hopefully this caution may carry over to closer consideration of Government activity in the area.

The evolution of biometric identity matching capacities

27. The current proposal is the next significant step in a national system that has been building though COAG towards a national biometric identification data base for over a decade.
28. In 2007 COAG agreed to a National Identity Security Strategy (NISS) which was updated in 2012 with the establishment of a national Document Verification Service (DVS). A significant COAG initiative in 2012 was the creation of the National Biometric Interoperability Framework:

> *'to foster greater collaboration between Agencies using biometric systems across government. This Agreement marks an important step in implementing the National Biometric Interoperability Framework and in achieving the priorities of the NISS more broadly'* [9]

29. In 2018 we have the proposed creation of the interoperability hub in the Department of Home Affairs and the the addition of the National Driver Licence Facial Recognition Solution (NDLFRS) to the NISS.
30. The combined scope and capacity of this national identity matching framework will provide a far more powerful identification and surveillance tool than would have been delivered by the Australia Card. Yet the system is invisible and unknown to most of the population. No-one has to carry an identity card. People who have provided their personal information for drivers licences and other government issued identity documents for specified purposes are not aware of the further use of that information.
31. The CCLs noted that only 10 submissions on this Bill (including the CCL's) had been received by the PJCIS by the closure date. This may indicate indifference by the public. More likely it indicates the low profile and lack of public awareness of the Bill – and for some civil society organisations, the very tight timeline of a few weeks to make a submission.

Future scope and function creep

32. It is not likely that the evolution of this system will now cease. The CCLs suggest that the usual function and scope creep syndrome will most likely continue.
33. This will be particularly likely if the current wide and inappropriate discretion in relation to making new rules about the kind of identity information to be included and new identity matching services is left with the Home Affairs Minister and not the Parliament - and if the privacy protections and the independent oversight of the system are not significantly strengthened.

[9] COAG: Intergovernmental Agreement On Identity Matching Services October, 2017 p3

34. Most significantly, it is hard to believe that given the technological capability and the facial recognition national database necessary to deliver close to real time mass surveillance both exist, that the pressure for this capability to be used in many contexts will not be pushed and allowed.
35. Australians should be worried about that potential.

Home Affairs Department - Minister and Secretary

36. When powers are being legislated for the executive it is always essential to consider the implications of them being administered one day by a Government or a Minister lacking due respect for rights and liberties or judicial independence and build in appropriate protections.
37. The CCLs are concerned that the Home Affairs Minister is the responsible Minister for the major Identity-matching Services Bill - including the development and operation of the enhanced interoperability hub and the NDLFRS database and other discretionary powers.
38. It is a controversial scheme with significant implications for rights and liberties. The history the Minister's approach to Immigration and Border Protection may not inspire community confidence that these rights and liberties would be appropriately protected if the identity matching services come under his responsibility.
39. There may also be similar concerns relating to the Secretary of the Home Affairs Department Michael Pezzullo. In this context we note our unease with the reported views of the Secretary of the Home Affairs Department Michael Pezzullo on the role of the state – (and he does appear to be speaking of the Australian state):

> *'The state has to increasingly imbed itself, not [be] majestically sitting at the apex of society dispensing justice', said Pezzullo. 'The state has to imbed itself invisibly into global networks and supply chains, and the virtual realm in a seamless and largely invisible fashion, intervening on the basis of intelligence*

and risk settings, increasingly at super-scale and at very high volumes'[10].

40. Understandably this speech has been much quoted. We accept this is an extract from a longer speech – but these words would be disturbing if they came from the head of an intelligence agency which one expects to work in secrecy in many contexts. They are confronting and particularly disturbing when coming from the Secretary of the powerful Home Affairs portfolio about to have its powers and responsibilities for the national identity matching services significantly increased.
41. The CCLs consider that the powerful identity matching and surveillance tools provided by the huge national facial recognition identity database and the technical matching capacity of the interoperability hub should be located in the Attorney Generals Department and that the AG should be the relevant Minister responsible for this legislation.
42. Regardless of its location, it is absolutely essential that the amendments to the Bill proposed in our submission[11] to remove the Minister's wide and inappropriate discretion to make new rules relating to the service, and the provision of stronger oversight and accountability provisions including more frequent independent reviews be acted on.

Joint CCLs View and Recommendations

43. **The CCLs reiterate their considered view** that this further development of a national facial recognition data base and an enhanced interoperability hub will together provide the capacity for mass surveillance of the population by the state and will have, over time, significant damaging implications for the nature of our society and the robustness of our democracy.

[10] Michael Pezzulo Secretary of Home Affairs portfolio speech to Trans-Tasman Business Circle 17 Oct 2017. Quoted by Stephen Easton : '*The case for a Department of Home Affairs: Pezzullo on his place in history'* in The Mandarin 16/10/2017
[11] [JCCLs PJCIS submission number 9] All Recommendations in this submission are relevant to this additional recommendation.

Recommendation 1

44. **The CCLs oppose** the passage of *The Identity-matching Services Bill 2018* as currently drafted for its potential to allow real time mass surveillance of the Australian public with the inevitable result of a chilling effect on public protest and dissent.

Recommendation 2

45. **The CCLs recommend** that Ministerial responsibility for the *Identity-matching Services* legislation (if passed) be changed from the Home Affairs Minister to the Attorney General.
46. **The Joint CCLs reiterate their support** for the detailed recommendations made in their prior submission to the PJCIS on these Bills.

Concluding comments

47. The CCLs hope this supplementary submission assists the Committee in its review of these Bills.
48. This submission was written on behalf of the Joint Councils for Civil Liberties by Dr Lesley Lynch (Vice President NSWCCL) and Tim Warne (Chair, Privacy Workgroup, Liberty Victoria) with input from the Executives of the other Joint CCLs.

Therese Cochrane
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission
Dr Lesley Lynch Vice President
NSWCCL