Submission No 4

INQUIRY INTO ROAD TRANSPORT AMENDMENT (NATIONAL FACIAL BIOMETRIC MATCHING CAPABILITY) BILL 2018

Organisation: NSW Council for Civil Liberties

Date Received: 5 November 2018

New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

NSW Legislative Council Standing Committee on Law and Justice Inquiry

NSW Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018

2nd November 2018

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts; attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018

1. The NSW Council for Civil Liberties *(NSWCCL)* welcomes the opportunity to make a submission to the Standing Committee on Law and Justice (*the Committee*) on its inquiry into the provisions of the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 (*RTA Bill*).

2. We agree that it is a primary responsibility of the state to protect public safety and we support police, security and intelligence agencies having appropriate powers and resources to carry out this role as effectively as possible – with the caveat that these powers are consistent with the maintenance of a robust democracy and do not unwarrantedly undermine the rights and liberties of its citizens.

SECTION 1: BACKGROUND TO THE RTA BILL

3. On 5 October 2017, Federal, State and Territorial leaders agreed to establish a National Facial Biometric Matching Capability (*Face Matching Service*) and signed the Intergovernmental Agreement on Identity Matching Services (*IAIMS*), to implement it. The resulting Identity-matching Services Bill 2018 (*Cwlth*) (*the Commonwealth Bill*) if implemented will facilitate the exchange of identity information between the Commonwealth and State and Territory governments, pursuant to the IAIMS.

4. The NSW Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 (*RTA Bill*) will amend the Road Transport Act 2013 (*RTA*) to allow Roads and Maritime Services to contribute NSW driver licence facial images and associated personal information for searching within the Face Matching Service. It also permits an "authorised government agency" to collect, keep and use photos and associated personal information from the Face Matching Service.

5. The NSWCCL - jointly with other civil liberties bodies across Australia - made two submissions to the Parliamentary Joint Committee on Intelligence and Security on the Commonwealth Bill raising many detailed concerns about the Bill and a more fundamental concern about the broad implications of the proposed national identity database and the associated face matching capabilities.[1]

6. NSWCCL's broad concerns about the long-term implications of the Commonwealth Bill's

[1] Joint Councils for Civil Liberties submission (21/3/2018) and supplementary submission (31/3/2018) to the Parliamentary Joint Committee on Intelligence and Security on The Identity-Matching Services Bill 2018 and The Australian Passports Amendment (Identity-Matching Services) Bill 2018. Submissions 9 and 9.1 https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IMSBill/Submissions

proposed significant expansion in the national identity matching services framework are relevant to the consideration of the cognate NSW Bill and we therefore restate these concerns before responding more specifically to the NSW Bill.

SECTION 2: THE BROAD CONTEXT AND LONG-TERM IMPLICATIONS

7. Given the agreement 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 the Commonwealth Bill will eventually be passed by the Australian Parliament - as will some version of the cognate NSW Bill be passed by our State Parliament. It is our hope that an understanding of the broader context and likely long-term implications will encourage the Government and Parliament to give very close consideration to the protections for both privacy and for the maintenance of a healthy democratic society that should be included in both the Commonwealth and the NSW legislation.

8. The Australian Government and the Explanatory Memorandum for the Commonwealth Bill seem to suggest that nothing much would be changed by the legislation beyond enhanced speed and efficiency for law enforcement and intelligence agencies[3]. NSWCCL agrees 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.

9. The current enhancement proposal however 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.

Public political discourse and protest

10. 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.

11. 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.

12. 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,

[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] *The Identity-matching Services Bill 2018; Explanatory Memorandum. P2*

railway stations, shopping centres etc) we are effectively killing anonymity.

13. (The Prime Minister 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[4].**)**

14. 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.

15. There is no shortage of well documented modern history on the longer-term incompatibility of the surveillance state and democracy.

Recent historical context for national identity systems

16. 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. In 1987 and in 2006 the Federal Government attempted to implement national identity schemes – most memorably, the Australia Card and then the Access Card.

17. 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. Neither was implemented and it was reasonable to assume that, given the strength of community opposition, future Governments would be wary of trying again.

18. 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.

19. 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.

20. 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.

[4] ABC PM 5/10/2017

The evolution of biometric identity matching capacities

21. 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. 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'[5]

22. In 2018 we have the proposed creation of the interoperability hub in the Department of Home Affairs and the addition of the National Driver Licence Facial Recognition Solution (NDLFRS) to the NISS.

23. 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 driver's licences and other government issued identity documents for specified purposes are not aware of the further use of that information.

Future scope and function creep

24. It is not likely that the evolution of this system will now cease. NSWCCL suggests that the usual function and scope creep syndrome will most likely continue. 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.

25. 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.

26. Australians should be worried about that potential.

[5] COAG: Intergovernmental Agreement on Identity Matching Services October, 2017 p3

SECTION 3: DETAILED COMMENT ON THE RTA BILL

27. NSWCCL's major problem with the RTA Bill is that the Commonwealth Bill is flawed and inconsistent with the agreement made with the States and was subject to strong criticism on these fronts. At this point in time we do not know if the Commonwealth Bill is to be amended or not to address these serious flaws and inconsistencies. Indeed, the PJCIS has not yet completed its report on its review of the Commonwealth Bill[6].

28. It seems premature to pass cognate legislation at a State level when the precise parameters of the Face Matching Service and much other detail, have not been settled within the main legislation. We note that Victoria and the ACT have not tabled corresponding draft legislation, reportedly because of privacy concerns - in particular the sharing of information with non-government bodies.[7]

Recommendation 1

The NSWCCL recommends that the RTA Bill should not proceed until the Commonwealth Bill is enacted into law.

Inconsistencies between the Commonwealth Bill and the IAIMS

29. The IAIMS and the Commonwealth Bill differ in a number of respects. Some of these inconsistencies are outlined below.

30. The IAIMS stated that a private sector organisation must have a legislative basis or authority to access Face Verification Services (*FVS*).[8] However, the Commonwealth Bill states that local government and non-government entities can use all identity matching services, if "verification of the individual's identity is reasonably necessary for one or more of the functions or activities of the local government authority or non-government entity."[9] This is very open-ended.

31. It is a watered-down version of what was promised and broadens access to the Face Verification Services. Under the broad purpose of verifying the identity of an individual[10] the local government might, for example use the services to issue parking tickets. There is a danger also that the Service could be used for pre-emptive identification of alleged or future criminals. For example, some businesses in the UK are sharing CCTV images with police and being notified of persons likely to shoplift.[11]

---

[6] The Commonwealth Bill was referred to the PJCIS for review on the 2nd March 2018. Submissions to that review formally closed on 21st March 2018 – though late submissions were accepted.

[7] Carey, A. (2 May 2018) "Biometrically opposed: Victoria queries Peter Dutton over facial recognition scheme" The Age, < https://www.smh.com.au/politics/federal/biometrically-opposed-victoria-queries-peter-dutton-over-facial-recognition-scheme-20180502-p4zcvs.html>; accessed 26 October 2010

[8] Cls 4.9 and 5.3 IAIMS

[9] ss.7(3)(a) and 10 (2) Commonwealth Bill

[10] (s.6(8)) Federal Bill

[11] 'Facewatch "Thief Recognition" CCTV on Trial in UK Stores', BBC News (online), 16 December 2015 <http://www.bbc.com/news/technology-35111363> in Mann, Monique; Smith, Marcus --- "Automated Facial

32. The IAIMS stressed that the Commonwealth would be guided by the principle of maintaining "robust privacy safeguards", developed in consultation with Federal and State Privacy Commissioners. Participating agencies were to "implement appropriate security and access controls". These privacy safeguards are not outlined in the Commonwealth Bill. The Commonwealth Bill should be amended to include them. In their absence from the Commonwealth Bill, the RTA and the RTA Bill need to provide those privacy safeguards.

33. The IAIMS promised a public register of arrangements for sharing identity information which ideally would provide information as to the key elements of processing, including the purposes of the processing, type of data, duration of processing, rights of the individual to access or rectify their data. This provision is not in the Commonwealth Bill. It should be amended to include an appropriate public register.

34. The IAIMS stated that the Face Recognition Solution "will not hold information that is not reasonably necessary to support identity matching"[12]. There is no commitment to limiting data retention in the Commonwealth Bill or the RTA Bill.[13] Although s12 of the Privacy and Personal Information Protection Act 1998 NSW (*PPIPA*) deals with data retention there are exemptions from the principles.

35. The Commonwealth Bill expands federal powers beyond what was originally agreed by the States in the IAIMS. The NSW Government should be urging the Federal Government to amend the Commonwealth Bill to incorporate the safeguards in the agreement made with the States and resolve other inconsistencies.

36. If the Federal Government fails to significantly amend the Commonwealth Bill, the NSW Government should consider whether RTA Bill should be amended to include appropriate safeguards. As it stands the RTA Bill – and the Minister's second reading speech- are silent on these matters.

Recommendation 2

The NSWCCL recommends that RTA Bill should not proceed until major anomalies between the IAIMS and current Commonwealth Bill are resolved by their inclusion in an amended Commonwealth Bill.

---

37. The Joint CCL's submission to the PJCIS discusses in detail the weaknesses in the Commonwealth

---

Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSWLawJl 6; (2017) 40(1) University of New South Wales Law Journal 121
< http://www.austlii.edu.au/au/journals/UNSWLJ/2017/6.html>

[12] IAIMS, clause 6.16(a)

[13] In the 2015 Privacy Impact Assessment of the Interoperability Hub, the AG confirmed that the minimum amount of such data required for its purposes would be collected. (*2015 PIA)* <https://www.homeaffairs.gov.au/crime/Documents/agd-response-privacy-impact-assessment.pdf. accessed 25 October 2018

Bill and recommends a significant number of amendments to address the identified problems.[14] In the context of consideration of the RTA Bill we draw attention to some of those weaknesses which we think the NSW Government should be concerned about.

Robust privacy safeguards and privacy impact assessments

38. In the second reading speech of the RTA Bill[15] the NSW Attorney General stated:

> *"I reiterate previous statements from the New South Wales and Commonwealth governments that the capability has been designed and built with robust privacy safeguards in mind, has been subject to detailed privacy impact assessments and data security assessments, will only be accessible by authorised agencies and by individuals within those agencies who are also appropriately authorised and have undertaken required training, and will be subject to a robust compliance framework and independent oversight at both the New South Wales and national level. I commend the bills to the House."*

39. This assurance leaves a number of unanswered questions as neither the 'robust privacy safeguards' nor the 'robust compliance framework' are adequately embedded in the Commonwealth Bill. There are also weaknesses in the State privacy framework.

40. As stated previously, the IAIMS stressed that the Commonwealth would be guided by the principle of maintaining "robust privacy safeguards", developed in consultation with Federal and State Privacy Commissioners.[16] However, some Australian Government agencies, including the intelligence agencies, are completely exempt from compliance with the Privacy Act.[17]

41. At the State level, the Privacy and Personal Information Protection Act 1998 permits information exchange and limits or exempts compliance with IPP principles in many situations.[18] Evidence of robust privacy safeguards is therefore scant and lacking in detail.

42. The RTA Bill refers to the collection and release of "personal information".[19] The Commonwealth Bill specifically permits the collection of sensitive information, although racial or ethnic origin, health information and genetic information are exceptions to identification information. However, incidental collection, use or disclosure is permitted.

43. Biometric information, by its nature, captures information about a person's health, ethnicity and race and for that reason has been linked to inappropriate profiling. The risk exists that information provided for a specific purpose will subsequently become available for secondary purposes for which consent may or may not have been obtained.

---

[14] Joint CCLs submission to PJCIS 21/318.Sub 9.

[15] Second Reading Speech by the Attorney General of the Surveillance Devices Amendment (Statutory Review) Bill 2018, Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 and Terrorism (Police Powers) Amendment (Statutory Review) Bill 2018-Legislative Assembly Hansard – 17 October 2018

[16] IAIMS clause 2.1(a)

[17] As defined in the S. 7 Privacy Act 1988

[18] Division 3 The Privacy and Personal Information Protection Act 1998 (*PPIP Act 1998).*

[19] S4A PPIPA

44. The 2015 Privacy Impact Assessment suggested, amongst other things, regular audits of access and compliance provisions; a privacy government framework; and community engagement and complaint handling. It also recommended the federal Attorney General or an independent body approve an agency's eligibility to access the Face Recognition Service, and for agencies to have a safety net to support individuals adversely affected.

45. These are measures that should be required in the legislation and not left to be promulgated under rules.

Recommendation 3

The NSWCCL recommends The RTA Bill should not proceed until the Commonwealth bill is amended to include additional measures to ensure robust privacy safeguards and a robust compliance framework - including transparency, audit trails, independent vulnerability tests and mechanisms for responding to public complaints.

Data security assessments

46. The recent hacking of a national security contractor, has again demonstrated how easily the security of systems may be compromised and personal information acquired for illegal or malicious purposes.[20] Our governments do not have the resources or expertise to adequately compete with the private sector or combat unauthorised hackers.

47. Although identity theft is a threat to privacy when it involves the theft of someone's identity, new systems inherently increase the possibility of covert or illegal collection, storage and processing of sensitive material. Facial identity information is unique data tied to an individual's biological existence. It cannot be replaced, as one might a credit card and the potential exists for an individual to be compromised for life. [21]

48. IAIMS promised use of appropriate cryptographic technology and organisational, procedural measures in the processing, transmission and storage of biometric information. The 2015 PIA promised that the "minimum amount of such data required for these purposes will be collected."

Recommendation 4

The NSWCCL recommends the RTA Bill should not proceed until the NSW Government is satisfied that the Face Matching Service incorporates effective oversight and robust cryptographic protection

[20] Conifer, D (10 October 2017) "Defence contractor's computer system hacked, files stolen, cyber security report reveals" ABC News, accessed 17 Nov 2017, <mobile.abc.net.au/news/2017-10-10/defence-contractors-fles-stolen-in-hacking:-security-report/9032290>

[21] Article 29 Data Protection Working Party- European Commission "Opinion 3/2012 on developments in biometric technologies" 00720/12/EN , retrieved 7 October 2017 < http://ec.europa.eu/justice/data-protection/index_en.htm>, (*DPWP*) p.9; Froomkin, A.M. (2000) "The Death of Privacy?" Stanford Law Review, Vol 52, No.5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? Pp 1461-1543 at p.1495

against accidental or unauthorised interception, access or disclosure of biometric information in its data bases.

Access of non-government and local government entities

49. The Commonwealth Bill provides the Minister with discretion to make rules in relation to a request from a local government authority or non-government entity, for the purpose of using the identity matching service to verify an individual's identity. Access by non-government entities is of particular concern as there is very little detail in the Commonwealth Bill about who will be able to access this information and for what identification purposes.

50. The 2015 PIA recommended, and it was accepted, that: users be disabled and reauthorised every 3 months; auditing of access should take place regularly and access should be limited to a few law enforcement agencies (not service delivery agencies).

51. The RTA Bill permits an "authorised government agency" to collect from and release to the Face Matching Service, photographs and personal information. Authorised government agency includes the Authority (Roads and Maritime Services) or any agent of the Authority. This is a potentially wide group of contractors and non-government organisations.

Recommendation 5

The NSWCCL recommends that non- government entities should not have access to the identity matching services and the Commonwealth Bill should be amended to delete reference to them.

Recommendation 6

The NSWCCL recommends that the Commonwealth Bill be amended to:

(i) limit the access of local government bodies to all identity matching services to those functions or activities which are tightly aligned with a community protection activity as defined in the Bill[22]

(ii) strengthen the current benchmark for access by local government to all identity matching services (*"verification of the individual's identity is reasonably necessary for one or more of the functions or activities of the local government authority or non-government entity."*S7(3)(a)) by the deletion of the word '*reasonably*'.

Recommendation 7

The NSWCCL recommends that the NSW Government review the implied inclusion of 'any agent of the Authority' (Roads and Maritime Services) with the view of ensuring that inappropriate entities are not potentially provided access to the face recognition service.

Independent oversight at NSW and national level

52. The Commonwealth Bill provides for identification information and identity-matching services to be "prescribed by the rules." More generally the Minister may make rules as permitted by the

[22] S6ss(2)(3)(4)(5) Commonwealth Bill

Act or necessary or convenient to giving effect to the Act. At both the Federal and State level, making rules prescribing such important decisions means that many administrative processes are being made outside the legislative framework.

53. It is well accepted that the rules which have a significant impact on individual rights and liberties should be included in primary legislation.[23] By deferring these important decisions to delegated legislation and eliminating barriers to data sharing, the level of scrutiny of these processes is reduced, because there is little parliamentary oversight. The Face Matching Service is being introduced through administrative processes and is occurring outside of a legislative framework, and the increased scrutiny that entails.

54. The Commonwealth Bill does provide that the Information Commissioner and the Human Rights Commissioner are to be consulted before rules are made in regard to identity information services. However, there is no well-resourced, independent third party who can respond to the interests of individuals affected by the collection, use and sharing of biometric information, as recommended by the 2015 PIA. An independent third party should be appointed under the RTA Bill.

55. The collection and release of the private information of individuals will have "a broad impact on individuals who pose no threat to a legitimate government interest and therefore the state's burden to justify the restriction" is high.[24] It is for this reason also that any such legislation, State or Commonwealth, should be subject to regular review by an independent and impartial judicial authority. The Commonwealth Bill provides for a review of its operation by the Minister only within 5 years of its commencement. Annual reporting to the Minister provides mostly statistical information. There is no requirement for specific independent review in the RTA Bill.

56. The necessity for information sharing in the Commonwealth Bill is justified as being in the legitimate interest of the government and that in such cases consent of the affected individual is not required.[25] This is quite often not the case when no real choice or alternative is offered and there is little or no opportunity to opt out (Drivers' only other alternative is to not receive a licence). Drivers licence recipients should receive detailed information about the use and collection of their information.

Recommendation 8

The NSWCCL recommends that the RTA Bill should not proceed until S30(2) of the Commonwealth Act is amended to ensure that rules which will have adverse effects on individual liberties or rights cannot be made by the Minister.

[23] https://www.alrc.gov.au/publications/justifications-delegating-legislative-power-0

[24] Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" UN Doc A/HRC/29/32 (2015), paragraph 35

[25] Identity-Matching Services Bill 2018, Explanatory Memorandum, Statement of Compatibility with Human Rights atp.40

Recommendation 9
The NSWCCL recommends the operation of the Commonwealth Bill subject to independent review every three years instead of the currently proposed five years.

Recommendation 10
The NSWCCL recommends the RTA Bill should be subject independent review every three years.

Recommendation 11
The NSWCCL recommends that RTA Bill be amended to include a provision ensuring that all reasonable steps be taken to notify applicants, obtaining new or renewing driver's licences, that their personal information will be collected for the purposes of biometric matching.

CONCLUDING COMMENTS

57. The NSWCCL hopes this submission is of assistance to the Justice and Law Standing Committee. Representatives of the Council will attend the public hearing scheduled for Wednesday the 7th November to further discuss the issues relating to the Bill and to answer any questions the Committee has in relation to this submission. We thank the Committee for the invitation to attend.

58. This submission was written by Michelle Falstein Convenor of the NSWCCL Privacy Action Group and Dr Lesley Lynch Vice President of the NSWCCL with research input from Michael Brull NSWCCL Policy Lawyer.