Submission No 7

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

Organisation: Australian Lawyers for Human Rights

Date Received: 5 November 2018

AUSTRALIAN LAWYERS FOR HUMAN RIGHTS

2 November 2018

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

www.alhr.org.au

Hon Natalie Ward MLC
Chair
Standing Committee on Law and Justice Legislative Council
NSW Parliament
Sydney
NSW 2000

By email: natalie.ward@parliament.nsw.gov.au, law@parliament.nsw.gov.au

Dear Chair

Inquiry into the provisions of the Road Transport Amendment (National Facial Biometric Matching Capability) Bill 2018 ('the NSW Bill')

Australian Lawyers for Human Rights (**ALHR**) appreciates the opportunity to provide this submission in relation to the Committee's Inquiry into the NSW Bill.

We would be grateful if this submission could be taken into account despite it being sent to you after the closing time for submissions. We have only today become aware of the Inquiry and we note that the timeframe for submissions was very short, despite the importance of the matters in question.

1. Summary of Concerns

Relationship with problematic Federal Bills

1.1 The NSW Bill which is the subject of your Inquiry responds to the *Intergovernmental Agreement on identity-matching* entered into in October 2017.

1.2 Under the NSW Bill, the drivers' licence (and presumably non-driver identity card) information held by the NSW Government is to be provided to the Federal Government for use in the Federal Government's new 'information hub' (also known as the 'capability' in the NSW Bill) in accordance with Federal legislation.

1.3 However the proposed Federal legislation, being the *Identity-Matching Services Bill 2018* (**IMS Bill**) and the *Australian Passports Amendment (Identity-Matching Services) Bill 2018* (the 'Federal Bills') is **deficient in many areas** and has the potential to severely impact the human rights of all Australians. The Federal Bills exempt the Federal Government from the normal operations of the Australian privacy principles and allow individuals' personal and sensitive information, including biometric data to be used for any purpose the Federal Government may wish. **The Federal Bills do not respect privacy but enable surveillance and exploitation. NSW residents should not be made part of these arrangements.**

1.4 Numerous other bodies have expressed similar concerns to those described in this submission in relation to the Federal Bills including the Law Council of Australia, the Human Rights Commission,[1] Civil Liberties Australia, Joint Council for Civil Liberties, Queensland Council for Civil Liberties, the Australian Privacy Foundation and the Human Rights Law Centre[2].

Lack of public consent

1.5 What is of particular concern to most commentators is that these arrangements are being advanced by Federal and State Governments with no real public consultation, despite the well-known opposition of a majority of Australians to any national identity card system. The NSW Bill and Federal Bills, if enacted in their present forms, will result in a system far more draconian and invasive, and far more open to abuse, than any purely identity card system. ALHR submits that full public consultation and meaningful public consent is crucial. Australian and NSW citizens deserve no less. We have no opportunity to 'opt out' of this system which is being imposed with no public discussion. Citizen involvement, understanding and participation in important decisions, is an essential element of democracy. The decision to share individuals' personal information with the Federal Government, for use in unrestricted ways, is a crucial decision with far-reaching consequences both now and for future generations. In order for government to work for the public good, to be democratic, and to be seen to be operating in a transparent and democratic manner, citizens need to be consulted by government in relation to important decisions of this nature.

Less practical than existing arrangements

1.6 While we do not necessarily disagree with the aim of allowing identity-matching services to be used by government where there is a question of wrongdoing (rather than for surveillance of innocent people), such services must be surrounded by safeguards. Insufficient safeguards have been adopted at Federal level, and no safeguards at all have been included in the NSW Bill. Private information of NSW residents will, under the proposed NSW Bill, be given to the Federal Government of the day with no restrictions whatsoever.

1.7 This is in the context where a leading IT expert, Dr Paul Henman of Queensland University, has submitted that the proposed Federal 'hub' holding drivers' licence information from 8 different jurisdictions will be both a more expensive and a less efficient system than leaving the drivers' licence information with the States and Territories and having those separate databases interrogated, if need be, from the Federal 'hub.'[3]

1.8 While we still maintain the concerns described in this submission in relation to the proposed Federal use of individuals' personal information, we agree with Dr Henman that there is less chance of hacking and more chance for State Governments to impose appropriate privacy restrictions on the use of their residents' information under Dr Henman's proposal – as opposed to what the Human Rights Law Centre calls a **'very high risk proposed regime'** on the part of the Federal Government.[4]

Safeguards required because identity matching doesn't always work correctly

1.9 The potential impacts on citizens' human rights might be of less concern if facial recognition software always worked correctly. However this is not the case, as discussed further below, and the negative impact on innocent people of being mis-identified as persons of suspicion is a real and important problem.

---

1 "Identity-matching bills threaten our rights" 3 May 2018, https://www.humanrights.gov.au/news/stories/identity-matching-bills-threaten-our-rights

2 See generally the Federal Inquiry Submissions page in relation to those Bills at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IMSBill/Submissions

3 Submission 19, Inquiry Submissions page

4 Submission 19, p 1, Inquiry Submissions page

Safeguards required because of the chilling effect on public assembly and free speech

1.10 Possible uses of biometric databases under the Federal Bills, note the Human Rights Law Centre, 'depart dramatically from the level of surveillance that has been undertaken [until now] in liberal democracies.' [5] As they explain:

> Facial recognition technology, particularly real-time facial recognition, risks transforming public space into a sphere where each person can be monitored and identified… [thus posing] a significant threat to freedoms of expression, association and assembly as they are enjoyed in Australia, which must be taken into account when the adoption and use of such technologies is being considered. [6]

Commercialisation of personal information

1.11 We are also strongly opposed to the concept that information obtained through or used by any government services could be made available for commercial purposes, which still seems to be highly probable under the Federal Bills.[7]

2 What can be done under the Federal Bills

2.1 Identity matching can be used for a range of purposes, some of which have a higher impact on privacy and civil liberties than others. For example, facial recognition software can be used (1) simply for confirmation of an image or an individual's identity (whereby an image is matched only against other images held in relation to one person) or (2) it can be used to compare a person's image against a whole database, in a search to identify the person. Will the images held by the Federal Government be used only for the first purpose (which is the implication from the Explanatory Memorandum) or could they be used for the second purpose as well? Will the images be searched on a targeted basis for individuals suspected of crimes? Or will there be continuous and generalised searches of the images of innocent people?

2.2 The problem is that the Federal Bills are deliberately phrased in general and open-ended terms, with no appropriate purpose-based restrictions. In its present form the IMS Bill allows dragnet searches without any warrant, with no accountability and no transparency. While sections 5(2) and (3) of the IMS Bill purport to respect privacy principles regarding sensitive personal information, in fact they enable the opposite, so long as the information gathered is not 'primarily' of a sensitive nature. That is, such information may be gathered and kept where it is obtained indirectly or collaterally, without any warrant, without the person concerned being informed, and with no restrictions or transparency as to how that information is used.

2.3 It is also worthy of note, as Valerie Heath has pointed out,[8] that the Federal Department of Home Affairs which is responsible for the 'hub' or the 'capability' is also the department with responsibility for CCTV systems which are being extended in many areas throughout Australia. The likelihood of facial identification being used on a mass scale by that Department, with the full database of images of innocent people being utilised rather than only the images relating to a particular individual suspected of wrongdoing, is therefore a real one.

2.4 The Federal Bill should be redrafted to make it clear how the personal information to be held by the Federal government will be used, before the NSW Bill can be properly considered. The Human Rights Law Centre has pointed to precedents in the legislation of other jurisdictions which restrict the use of facial recognition technology in situations where freedom of assembly or

---

5 Submission 16, p 6, at Inquiry Submissions page

6 Ibid, p 10.

7 Elise Thomas, "Coalition could allow firms to buy access to facial recognition data", 26 November 2017, *The Guardian Online*, at https://www.theguardian.com/technology/2017/nov/26/government-could-allow-firms-to-buy-access-to-facial-recognition-data

8 Submission to NSW Inquiry, 2 November 2018.

expression would be chilled.[9] The Federal Bill should similarly be drafted so as to specifically protect democratic freedoms and public activities.

3. ALHR's Human Rights Concerns

3.1 Pursuant to the principle of legality, Australian legislation and judicial decisions should adhere to international human rights law and standards, unless legislation contains clear and unambiguous language otherwise. Furthermore, the Australian parliament should properly abide by its binding obligations to the international community in accordance with the seven core international human rights treaties and conventions that it has signed and ratified, according to the principle of good faith.

3.2 ALHR endorses the views of the Parliamentary Joint Committee on Human Rights (PJCHR) expressed in Guidance Note 1 of December 2014[10] as to the nature of Australia's human, civil and political rights obligations, and agree that the inclusion of human rights 'safeguards' in Commonwealth legislation is directly relevant to Australia's compliance with those obligations.

3.3 Generally, behaviour should not be protected by Australian law where that behaviour itself infringes other human rights. There is no hierarchy of human rights – they are all interrelated, interdependent and indivisible. Where protection is desired for particular behaviour (such as right to collect and use peoples' personal and/or biometric information) it will be relevant to what extent that behaviour reflects respect for the rights of others – in this case the people whose information is being collected, used and perhaps sold. It is submitted that such behaviour fails the fundamental test of respecting the privacy and other human rights of the persons involved.

3.4 Legislation should represent an **appropriate and proportionate response** to the harms being dealt with by the legislation, and adherence to international human rights law and standards is an important indicator of proportionality.[11] Conversely, failure to adhere to such standards indicates that legislation is disproportionate and unacceptable.

4. Human rights impacted by the proposed Federal Bills to which the NSW Bill relates

4.1 The Explanatory Memoranda for the Federal Bills identify the following rights under the *International Covenant on Civil and Political Rights* (**ICCPR**) as potentially impacted, arguing however that the impact is proportionate, necessary and reasonable in the circumstances. These are:

- the right to privacy in Article 17 of the ICCPR
- the right to liberty and security of the person contained in Article 9 of the ICCPR
- the right to freedom of expression contained in Article 19 of the ICCPR.

4.2 In addition, it is submitted that:

- the *Identity-Matching Services Bill* will necessarily have a chilling effect upon the right of peaceful assembly in Article 21 of the ICCPR, and

---

9 Ibid, p 12.

10 Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, *Guidance Note 1*: *Drafting Statements of Compatability*, December 2014, available at <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources>, see also previous *Practice Note* 1 which was replaced by the Guidance Note, available at< https://www.humanrights.gov.au/parliamentary-joint-committee-human-rights>.

11 See generally Law Council of Australia, *"Anti-Terrorism Reform Project"* October 2013, <http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/a-z-docs/Oct%202013%20Update%20-%20Anti-Terrorism%20Reform%20Project.pdf> .

- the *Australian Passports Amendment* (*Identity-Matching Services) Bill 2018* may have an adverse impact upon the right of equal access to public service in Article 25 of the ICCPR and to equality before the law and equal protection of the law under Article 26 of the ICCPR.

4.3 Because Australia inherited the English common law, not a civil law system and did not adopt a bill of rights in its Constitution, Australia does not have a human rights framework to protect digital rights (including biometric data about identity). The Commonwealth *Privacy Act*[12] is very limited. There is no tort of privacy under Australian law and the common law offers a very inadequate protection for human rights such as privacy. In addition the common law can be overriden by contrary legislation. The result is a 'significant governance gap'.[13]

4.4 The Privacy Act regulates collection and use of personal information through thirteen 'Australian Privacy Principles' but does not address surveillance, which is permitted for law enforcement agencies under various legislation.[14] Nor does it apply to Commonwealth intelligence agencies[15] or State or Territory government agencies such as the NSW Police Force.[16] Some States have privacy legislation that regulates use of personal information by State and local government agencies,[17] in some cases involving criminal sanctions.[18]

4.5 Even where the Privacy Act does cover law enforcement agencies, there are many exemptions. And the *Privacy Act* provides for only limited civil redress, by way of complaints to the Australian

---

12 The Act applies to most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses– see https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10.

13 Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSW Law Jl 6; (2017) 40(1) *University of New South Wales Law Journal* 121, at 122.

14 The States have their own legislation. Relevant Commonwealth legislation includes: Part 5-1A of the *Telecommunications (Interception and Access) Act 1979 ('TIA Act')* (relating to data retention obligations), *the Telecommunications Act 1997, the Intelligence Services Act 2001,* the *Surveillance Devices Act 2004* and the *Australian Federal Police Act 1979* (Cth), s 60A(2) of which allows federal police recording and retaining of personal information. The AFP is legally permitted to collect facial images where it is 'reasonably necessary to fulfil its policing functions' and share them when it is 'reasonably necessary for law enforcement purposes' Attorney-General's Department (Cth), 'Face Matching Services' (Fact Sheet) 3 <https://www.ag.gov.au/ RightsAndProtections/IdentitySecurity/Documents/Fact-Sheet-National-Facial-Biometric-Matching- Capability.pdf>.

15 Not covered are: the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate, the Defence Intelligence Organisation, the Australian Geospatial-Intelligence Organisation. Office of the Australian Information Commissioner, "Which law enforcement agencies are covered by the Privacy Act?" at https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement.

16 Office of the Australian Information Commissioner, "Which law enforcement agencies are covered by the Privacy Act?" at https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement. It should be noted that the Australian Government Agencies Privacy Code (available at https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017) was registered on 27 October 2017 and comes into effect on 1 July 2018. It is a relatively short document which sets out specific requirements for government agencies to which the Privacy Act applies to assist them in adopting a best practice approach to privacy governance.

17 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Premier and Cabinet Circular No 12* (SA); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic); *Information Privacy Act 2014* (ACT); *Information Act* (NT).

18 Under s 62 of the *Privacy and Personal Information Protection Act 1998* (NSW) the unauthorised or corrupt use or disclosure by a public official of personal information obtained through their official functions is an offence punishable by up to 100 penalty units or imprisonment for up to two years.

Information Commissioner.[19]

5. Identity-Matching Services Bill 2018

5.1 There are several aspects of the *Identity-Matching Services Bill* which are of concern despite the references in the Bill to the application of the Australian Privacy Principles. These are:

- the purposes for which identity matching can be used
- who can access the information
- how they will keep the information secure
- how consent from individuals involved will be obtained

What will the information be used for?

5.2 It is a fundamental aspect of the *Australian Privacy Principles* that individuals should know the reason for collection of their personal information and that the information should be used only for that particular purpose or purposes. **This fundamental concept is not honoured** by the *Identity-Matching Services Bill,* which indeed specifically provides that data obtained for one purpose can be used for other purposes, with section 3 providing that: **'**The Department may use or disclose **for any of those purposes** information so collected (**regardless of the purpose for which it was collected**)' (emphasis added). The information may also be shared with other countries, amounting to a substantial breach of personal privacy.

5.3 ALHR submits that this ability to repurpose data results in a complete failure of transparency in relation to the data matching process and is highly undesirable. Persons affected need to be aware of the data being collected about them and should have to give a free and fully informed consent before that data can be used for a different purpose. (There are however problems around ensuring that any consent is both free and fully informed, as discussed further below).

5.4 In section 6 of the Bill, the various potential purposes for use of the identity-matching service are listed. It is concerning that many of the purposes relate not to uncovering of wrongdoing that has already occurred, but 'prevention' and 'promotion' activities - **which surely amount to ongoing surveillance and monitoring in the absence of any criminal offence having taken place**. **ALHR strongly objects to use of identity-matching services for these purposes, unless there is a clear connection to a likely offence.** Generalised monitoring is both ineffective (as it increases the size of the 'haystack') and a serious impact upon Australians' civil liberties. Are we becoming a police state that has identity- matching software operating in all public places including toilets[20] - no doubt at enormous public cost? The potential for authoritarian use of this legislation is obvious.

5.5 There is considerable evidence that the encouraging of surveillance, monitoring and investigations where there is no actual evidence of wrongdoing, is likely to result in discriminatory policing. The American Civil Liberties Union (ACLU) has recorded such results from similar US legislation. In its words (emphasis added):

> Using expanded authorities that permit investigations **without actual evidence of wrongdoing**, the FBI has also targeted minority communities for interviews based on race, ethnicity, national origin, and religion. It has used informants to conduct surveillance in community centers, mosques, and other public gathering places and against people exercising their First Amendment right to worship or to engage in political advocacy. And among America's minority communities, "flying while brown" soon joined "driving while black" as a truism of government-sanctioned discrimination and stigma. It's hard to overstate the damage done to the FBI's relationship with minorities, particularly American Muslims.[21]

---

19 Sections 36, 40, 52.

20 Agence France-Presse in Beijing, "From ale to jail: facial recognition catches criminals at China beer festival", The *Guardian Online*, 1 September 2017, at https://www.theguardian.com/world/2017/sep/01/facial-recognition-china-beer-festival

21 Ibid.

5.6 There is also evidence that identity-matching is a flawed and often inherently discriminatory process. As Professor Campbell notes:

> [In the UK,] South Wales Police is the national lead on facial recognition technology and received a £2.6 million UK Government grant to run a pilot scheme. SWP deployed the system of a private company called Neoface at 18 public gatherings between May 2017 and March 2018, after which concerns were raised about accuracy: "91% of matches—2,451—incorrectly identified innocent members of the public" (Big Brother Watch, 2018). [22]

5.7 The reality is that computer programmes and algorithms – such as are used for identity-matching - are not necessarily neutral and will reflect the intrinsic social biases of the programmers. 'Algorithmic bias,' it is noted, 'is now a widely studied problem that refers to how human biases creep into the decisions made by computers. The problem has led to gendered language translations, biased criminal sentencing recommendations, and racially skewed facial recognition systems.'[23] Studies in the US have already found evidence of bias in online advertising, recruiting,[24] facial recognition, bail and sentencing decisions[25] and law enforcement decision-making[26] all driven by purportedly neutral algorithms. Edwards and Veale observe that algorithmic systems trained on past biased data which introduce correlations based on race, religion, gender, sexuality, or disability without careful consideration are inherently likely to recreate or even exacerbate discrimination seen in past decision-making.[27] A risk of incorrect outcomes is therefore very real. Such outcomes will have serious and negative effects upon the lives of innocent Australians.

5.8 The possibility of politically-motivated surveillance under the Federal Bills is also very real.[28] As mentioned above, ALHR is concerned that:

(a) substantial current and potential infringements upon individuals' privacy rights are being made by both Federal and State governments in relation to the proposed 'interoperability hub' arrangements, thereby having a chilling impact upon on our privacy, our rights of assembly and freedom of expression, and

(b) at the same time a door is being left open for those same privacy infringements to be 'monetised' for commercial purposes (see section 10 which contemplates access to the Facial Verification Service or FVS by local councils and non-government entities).

---

22 Professor Liz Campbell, Monash University (Submission 20) p 3 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IMSBill/Submissions

23 James Avanitakis and Andrew Francis, 'Data ethics is more than just what we do with data, it's also about who's doing it**',** *The Conversation*, 22 June 2018, <https://theconversation.com/data-ethics-is-more-than-just-what-we-do-with-data-its-also-about-whos-doing-it-98010> and see generally Cathy O'Neill, *Weapons of Math Destruction*, Crown Books, 2016.

24 See for example Nanette Byrnes, 'Why We Should Expect Algorithms to Be Biased', *MIT Technology Review*, June 24 2016 at <https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/>.

25 Sam Corbett-Davies , Emma Pierson , Avi Feller and Sharad Goel, "A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear," *Washington Post*, 17 October 2016 at https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/?noredirect=on&utm_term=.ac8774d65032.

26 'Discriminating algorithms: 5 times AI showed prejudice' *New Scientist Magazine* 2 April 2018, updated 27 April 2018 available at https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/.

27 Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a right to an explanation is probably not the remedy you are looking for,' *Duke Law and Technology Review* No.1, p.28, <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr>.

28 Human Rights Law Centre, op cit, p 11 ff.

Legislation that should be protecting our privacy is instead allowing unlimited Federal surveillance and commercial exploitation.

5.9 In our view this duality of purpose:

- indicates a lack of good faith on the part of the government,
- calls into question the constitutional basis of the legislation, particularly section 10, and
- demonstrates that the legislation's impact upon the human right to privacy is disproportionate and that the legislation does not protect Australians' right to privacy to the maximum extent possible.

5.10 We note that in Britain, courts have ruled in accordance with international human law jurisprudence that it is unlawful for images of innocent people who have never been charged or convicted of any offence to be retained in police databases.[29] That outcome should apply in Australia too.

Who can access the information

5.9 ALHR is troubled that the Facial Verification Service described in section 10 of the Federal Bill which can be accessed by local councils and non-government entities. This could result in the sale of sensitive personal information for commercial purposes. While some purported protections are included in sections 7(3) (consent of individual) and 7(4) (application of Australian Privacy Principles) these protections would appear to be of little use in practice. Thus in order to be able to drive in NSW one must 'consent' to have one's photograph taken, and reproduced on one's driver's licence. In having our photos taken for our drivers licences – or for non-driving photographic identity cards - we are not intending to consent to our photos being used and sold by State and Federal Governments. Why is the State government assuming it has received our informed consent?

Who will keep the information secure?

5.9 This question is particularly relevant given the large numbers and types of entities which will be allowed to access any personal information about NSW residents which is held Federally. While the Explanatory Memoranda for the Federal Bills indicate that data will only be matched and personal information not be retained/ downloadable by any third party interrogating the Federal information 'hub', this appears to:

- be a practical matter which could be changed subsequently as there is no such limitation in the Federal legislation itself, and no restrictions in the NSW Bill;
- ignore the fact that for the data to be 'matched' the interrogator must themselves already have a facial image which they send in to be checked. The information must already be in existence both within and outside the 'hub' if it is to be checked. Thus while the interrogator may not receive a copy of the government's own data, the interrogator will still be able to keep a copy of their own data, whether it is confirmed by the hub to be a true image of the person in question or not.

---

29 Alan Travis, "Watchdog warns over police database of millions of facial images" *The Guardian Online*, 14 September 2017, at https://www.theguardian.com/world/2017/sep/13/watchdog-warns-over-police-database-of-millions-of-facial-images. Permanent retention of biometric material in non-conviction based databases has been found to breach the right to privacy and family life as provided for in Article 8 of the European Convention on Human Rights (*S v Marper* (2009) 48 EHRR 50, *S* v *United Kingdom* (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008 and *Reklos and Davourlis* v *Greece* (European Court of Human Rights, First Section, Application No 1234/05, 15 January 2009)) – see Inquiry submissions from Professor Liz Campbell, Monash University (Submission 20) p2 and Human Rights Law Centre (Submission 16), p 10, both at Inquiry Page, op cit.

5.10 The Federal Government itself does not have a good record of keeping personal sensitive information secure, contrary to the Australian Privacy Principles. In 2014 the Department of Immigration accidentally released the personal data relating to 10,000 asylum seekers.[30] And in 2016 the MBS/PBS dataset, containing health information about 10% of the entire Australian population, was released as 'de-identified' open data but was able to be decrypted so that doctors, and some of their patients, proved to be identifiable.[31] The Minister for Law Enforcement and Cyber Security estimated that in 2017 there were 734 cyber incidents in private sector systems affecting the national interest.[32]

5.11 According to Anna Johnston of Salinger Privacy:

> *A NSW auditor-general's report found that two-thirds of NSW government agencies are failing to properly safeguard their data, by not monitoring the activities or accounts of those with privileged access to data, and one-third are not even limiting access to personal information to only staff with a 'need to know'.*
>
> *Leaving aside the question of why the NSW Privacy Commissioner is not resourced adequately to undertake these audits instead of needing the auditor-general to look into data protection, this report highlights a disturbing lack of compliance with the Data Security principle, which is neither new (NSW privacy legislation turns 20 this year) nor rocket science.*
>
> *Ignoring the privacy risks posed by staff misusing data is naïve; when I think of the more than 300 privacy cases against NSW public sector agencies over the past two decades, I cannot think of one that has involved a complaint arising from a disclosure to hackers, but countless have involved staff misusing the personal information to which they were given access.* [33]

5.12 And when one comes to non-government APP entities, the picture is even bleaker. Non-government entities will effectively be encouraged by this legislation to keep their own private databases of facial records – for checking against 'the hub.' APP entities are not subject to regular oversight by the Regulator, which relies on voluntary compliance by APP entities with the *Privacy Act* and associated *Australian Privacy Principles*. Problems only come to light through private complaints or self-reporting of breaches. And Equifax, one of the approved gateway service providers for the existing and similar Australian Document Verification System, recently breached security on the personal details of over 143 million US citizens.[34]

5.13 The purported protection in section 7(4) for individuals having their identities checked by local government or non-government bodies (which is that the body will have entered into an agreement to abide by rules along the lines of the *Australian Privacy Principles*) really provides very little protection in practice, particularly where the agreement relates to biometric data which of itself removes one of the key APP rights – to be anonymous or pseudonymous.

---

30 Oliver Laughland, Paul Farrell and Asher Wolf, "Immigration Department data lapse reveals asylum seekers' personal details", *The Guardian Online,* 19 February 2014, at https://www.theguardian.com/world/2014/feb/19/asylum-seekers-identities-revealed-in-immigration-department-data-lapse.

31 Paris Cowan, "Health pulls Medicare dataset after breach of doctor details," 29 September 2016, IT News online, at https://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463 and Chris Culnane, Benjamin Rubinstein and Venessa Teague, "Understanding the Maths is crucial for Protecting Privacy", 29 September 2016, Pursuit, University of Melbourne, at https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy

32 Amy Remeikis, "Australia warns businesses about sophisticated cyberattacks", *The Guardian Online*, 10 October 2017 at https://www.theguardian.com/australia-news/2017/oct/10/australia-warns-businesses-about-sophisticated-cyberattacks

33 "Too much cyber, not enough privacy 101" by Anna Johnston, *Salinger Privacy*, 5 February 2018 at https://www.salingerprivacy.com.au/2018/02/05/not-enough-privacy-101/

34 Elise Thomas, op cit.

5.14 Organisations which collect sensitive data are required under APP 2 to give individuals the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. This principle does not apply if the APP entity is required or authorised by or under an Australian law, or by the order of a court or tribunal, to deal with individuals who have identified themselves; or it is impracticable for the APP to do so. Clearly, however, the use of physical biometric data matching removes the right of pseudonymity that individuals would otherwise have.

Obtaining consent from individuals

5.15 Section 7(3) requires consent to be given by individuals to the identity-matching (relevant to use of the service by local governments and non-government entities under section 10(2) – consent not otherwise being required). But what if your consent is a pre-condition to the provision of a service – whether obtaining your driver's licence (as in the case of the NSW Bill), having your rubbish removed, entering a shopping centre (number plates already being recorded in shopping centre car parks) or opening a bank account?[35]

5.16 To quote Anna Johnston again:

> 'there remains a problem with the 'notice and consent' model of privacy protection. As academic Zeynep Tufekci has noted, 'informed consent' is a myth: "Given the complexity (of data privacy risks), companies cannot fully inform us, and thus we cannot fully consent."
>
> Putting the emphasis for privacy protection onto the consumer is unfair and absurd. As Tufekci argues in a concise and thoughtful piece for the New York Times:
>
> "Data privacy is not like a consumer good, where you click 'I accept' and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices. A more collective response is needed."
>
> *The data is de-identified so there is nothing to worry about.*
>
> *If you don't like it, opt out.*
>
> *If you've done nothing wrong, you've got nothing to hide.*
>
> It's time to put those fallacies to rest. The US model of 'notice and consent' has failed. Privacy protection should not be up to the actions of the individual citizen or consumer. It's the organisations which hold our data – governments and corporations – which must bear responsibility for doing us no harm.
>
> They could start by minimising the collection of personal information, storing data securely, and limiting its use and disclosure to only directly related secondary purposes within the subject's reasonable expectations.'

We endorse those comments.

6. Conclusion

6.1 Any legislation which impinges upon human rights must be narrowly framed, proportionate to the relevant harm it addresses, and provide an appropriate contextual response which minimises the overall impact upon all human rights. ALHR is concerned that the Federal Bills do not strike the right balance and that NSW should not provide private personal information of NSW residents to be used for unspecified possibly commercial purposes by the Federal Government through 'the hub' or 'the capability'.

6.2 As the Human Rights Law Centre comments:

---

35 Elise Thomas, op cit, quoting Monique Mann, Australian Privacy Foundation.

> The use of biometric data should be governed by laws with sufficient detail for Australians to understand what is being done with their information in their name, and adequate safeguards to protect against 'function creep,' misuse of data and inaccuracy. If we are to override requirements for individual consent in the public interest, we need to know what that interest is and what evidence justifies new powers. We need meaningful parliamentary understanding and agreement to the proposed regime, which is virtually impossible given the absence of detail in the Bill. We are troubled by the practice – exemplified by this legislation – of seeking broad authorisations to engage in open-ended activities with the specifics of new powers left to rules or policies to be developed by Ministers and their agencies.[36]

6.3 ALHR is disturbed that the Federal Bills will severely impact on the privacy and other human rights of Australian individuals and involve the use of citizens' biometric data for surveillance and commercial purposes. The NSW Bill involves the giving up of information to the Federal government without the consent of NSW residents and without any meaningful privacy protections being negotiated by the NSW Government for its residents.

ALHR is happy to provide any further information or clarification in relation to the above if the Committee so requires.

If you would like to discuss any aspect of this submission, please email me at:

Yours faithfully

Kerry Weste

President

Australian Lawyers for Human Rights

ALHR was established in 1993 and is a national association of Australian solicitors, barristers, academics, judicial officers and law students who practise and promote international human rights law in Australia. ALHR has active and engaged National, State and Territory committees and specialist thematic committees. Through advocacy, media engagement, education, networking, research and training, ALHR promotes, practices and protects universally accepted standards of human rights throughout Australia and overseas.

---

[36] Op cit, p 2.