AUSTRALIAN LAWYERS FOR HUMAN RIGHTS

20 March 2018

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

www.alhr.org.au

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

By email: pjcis@aph.gov.au

Dear Committee Secretary

Inquiry into the provisions of the Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018

Australian Lawyers for Human Rights (**ALHR**) is grateful for the opportunity to provide this submission in relation to the Committee's current Inquiry into the Bills.

We note that the time frame for considering these Bills is particularly short and fails to allow for adequate consultation on legislation that has the potential to impact the human rights of all Australians. There may well be other issues in relation to the Bills which we have failed to identify but which are also of importance.

While we do not disagree with the aim of allowing identity-matching services to be used by government, such services must be surrounded by safeguards and it is not clear that sufficient safeguards have been adopted. We are also strongly opposed to the concept that information obtained through or used by these government services could be made available for commercial purposes.[1]

Table of Contents

[1] 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

1. ALHR

1.1 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.

2 Summary of Concerns: 'too much cyber, not enough privacy'[2]

2.1 Following on from the principles explained in the previous section, our concern in relation to the *Identity-Matching Services Bill 2018* is that **substantial infringements upon individuals' privacy rights are being given away by government in the name of security**, but at the same time a door is being left open for those same privacy infringements to be 'monetised' for commercial purposes. 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, 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.

2.2 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 include:

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

These issues are discussed further below in section 5.

2.3 Our concern in relation to the *Australian Passports Amendment* (*Identity-Matching Services) Bill 2018* is that a distinction needs to be drawn between the Minister using a computer programme to assist him or her in making a decision (which might be appropriate), and the Minister leaving the decision entirely to the computer programme.

2.4 This latter course in our view arguably amounts to a dereliction of duty and an *ultra vires* attempt to delegate a discretion, because surely a discretion can only be delegated to a human being themselves capable of exercising real and genuine consideration of an issue (*Fay v Moramba Services Pty Ltd* [2010] NSWSC 725 at [34]–[40]; *Re Baden's Deed Trusts; McPhail v Doulton* [1971] AC 424 at 449; [1970] 2 All ER 228 at 240) with 'a fair consideration of the subject' (*Re Beloved Wilkes's Charity* (1851) 42 ER 330). **We are not convinced that the proposed delegation to a computer programme is either appropriate or legally correct and believe that the proposed section would result in a situation that arguably breaches Ministerial fiduciary duties.**

2.5 Our argument is strengthened by the fact that the proposed section 56A itself contemplates that the computer programme might come to the wrong conclusion and that the Minister might need to reverse the programme's 'decision.' It is clear therefore that the legislation itself acknowledges the fallibility of a computer programme. We discuss this issue further below in section 6.

---

[2] See "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/

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[3] 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 it will be relevant to what extent that behaviour reflects respect for the rights of others.

3.4 It is only through holding all behaviours up to the standard of international human rights that one can help improve and reform harmful and discriminatory practices.

3.5 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. [4]

4. Human rights impacted by the proposed Bills

4.1 The Explanatory Memoranda for the 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
- 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

---

3 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> accessed 16 January 2015, 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>.

4 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> .

digital rights (including biometric data about identity). The Commonwealth *Privacy Act*[5] 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'.[6]

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.[7] Nor does it apply to Commonwealth intelligence agencies[8] or State or Territory government agencies such as the NSW Police Force.[9] Some States have privacy legislation that regulates use of personal information by State and local government agencies,[10] in some cases involving criminal sanctions.[11]

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 Information Commissioner.[12]

---

5 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.

6 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.

7 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>.

8 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.

9 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.

10 *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).

11 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.

12 Sections 36, 40, 52.

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

Purposes

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[13] - no doubt at enormous public cost?

5.5 As mentioned, **ALHR is concerned that substantial infringements upon individuals' privacy rights are being given away by government in the name of security**, but 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).

5.6 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.

---

13 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

We note that in Britain, courts have ruled 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.[14]

Who can access the information

5.7 ALHR is particularly concerned about the Facial Verification Service described in section 10 which can be accessed by local councils and non-government entities. This opens the gateway to 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 may be of little use in practice, as discussed elsewhere in this submission.

Who will keep the information secure?

5.8 This question is particularly relevant given the large numbers and types of entities which will be allowed to access the information. While the Explanatory Memoranda indicate that data will only be matched and personal information not be retained/ downloadable by the party interrogating the 'hub', this appears to:

- be a practical matter which could be changed subsequently as there is no such limitation in the legislation itself;
- 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.

5.9 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.[15] 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.[16] 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.[17]

5.10 According to Anna Johnston of Salinger Privacy:

---

14 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

15 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.

16 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

17 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

> *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.* [18]

5.11 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.[19]

5.12 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.

5.13 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

5.14 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, having your rubbish removed, entering a shopping centre (number plates already being recorded in shopping centre car parks) or opening a bank account?[20]

5.15 To quote Anna Johnston again:

---

18 "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/

19 Elise Thomas, op cit.

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

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.

6. Australian Passports Amendment (Identity-Matching Services) Bill 2018

6.1 ALHR notes that the ability of Ministers to delegate decisions to computer programmes is already well entrenched in legislation,[21] as is the ability of all parts of government to use computer programmes to assist in decisions on day to day matters, even including important issues such as risk assessments of refugee claims.

6.2 The problem is of course that a computer programme is only as good as the programme design and the information put into it. The proposed section 56A itself contemplates that the computer programme might come to the wrong conclusion and that the Minister might need to reverse the programme's 'decision.' It is clear therefore that the legislation itself acknowledges the fallibility of a computer programme. A computer is not capable of itself adding extrinsic facts to moderate the information it receives. It cannot take account of community values and expectations, considerations of fairness or common sense[22]. At the same time, understanding is growing that computer programmes, algorithms, etc will however reflect the intrinsic social biases of the programmers and are not necessarily as neutral as claimed. A risk of resultant incorrect, unfair or arbitrary decisions is therefore very real.

6.3 Nor are computer programmes coded by persons who understand how to interpret the laws that the programmes are meant to be following. It is not just a matter of reproducing the legislation, but of including the common law presumptions that underlie the legislation and the effects of the case law that has refined interpretation of the legislation. As Justice Melissa Perry of the Federal Court says:

---

21 Simon Elvery, "Howe algorithms make important government decisions – and how that affects you", 21 July 2017, ABC News online, http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858

22 The Honourable Justice Melissa Perry, "iDecide: the Legal Implications of Automated Decision-making", *Cambridge Centre for Public Law Conference 2014: Process and Substance in Public Law*, 15-17 September 2014, http://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20140915

> Through the process of translating laws into code, computer programmers effectively assume responsibility for building decision-making systems that translate policy and law into code. Yet computer programmers are not policy experts and seldom have legal training. How can we be sure that complex, even labyrinthal, regulations are accurately transposed into binary code? Even lawyers and judges frequently disagree on meaning, and the process of statutory construction itself is not only concerned with the ordinary meaning of words. Laws are interpreted in accordance with statutory presumptions. Meaning is also affected by context. Apparent conflicts between statutory provisions may need to be resolved. And the hierarchy between provisions determined. These are not necessarily simple questions and the potential for coding errors is real.[23]

6.4 The Robodebt debacle provides a clear example of reliance on a bad programme (and a bad system). Centrelink requires reporting of employment income, including casual employment and overtime payments, for fortnightly periods which include several days in the future from the reporting date. The system does not allow you to wait for your pay slip so you can give the accurate figures in retrospect. This practice therefore inevitably requires the Centrelink recipient to go back and correct the data when it turns out that they have been paid for more or fewer hours than they estimated would occur. As has been well publicized, access to a Centrelink officer is very difficult and thus attempting to report new data is also very difficult and time consuming. How could there not be problems with automatic debt assessments in such a situation?

6.5 Thus problems can easily arise with the efficacy of computer programmes. An additional problem is that their use is not transparent, and it can be difficult to identify how it is that, or whether or not, a computer programme has made a wrong decision. Administrative processes need to be transparent so that the decision-makers can be accountable.[24] To quote Justice Perry:

> errors in computer programming and in the translation of complex laws into binary code can result in wrong decisions potentially on an enormous scale if undetected. Input errors may also lead to flawed decisions. Nor are all decisions by government of such a nature that they can appropriately or fairly be made by automated systems. The use of these systems by governments therefore raises questions as to the measures necessary to ensure their compatibility with the core administrative law values or principles that underpin a democratic society governed by the rule of law, in particular:
>
> - to ensure the legality of purported actions by public bodies;
> - to guard against the potential erosion of procedural fairness; and
> - to safeguard the transparency and accountability of government decisions by the provision of reasons and effective access to merits and judicial review.[25]

6.6 Justice Perry notes that programming errors may be replicated across many thousands of decisions undetected, and not until the outcomes reach catastrophic proportions will they be noticed (as with the Robodebt scenario). Where failures are less catastrophic, and thus less noticeable, the system's incorrect decisions may well remain hidden.[26]

6.7 Our concern in relation to the *Australian Passports Amendment* (*Identity-Matching Services) Bill 2018* is that a distinction needs to be drawn between the Minister using a computer programme

---

23 ibid

24 ibid

25 Ibid, see also Dominique Hogan-Doran SC, "Accountability Mechanisms: Part III: Automated Decision-making", 25 February 2017, *Law Council of Australia 2017 Immigration Law Conference*, at https://static1.squarespace.com/static/568c9f234bf1182258eb9fbc/t/58b803cf37c58149faf5a5a7/1488454608349/Accountability+Mechanisms+Beyond+Merits+Review.pdf

26 Perry, op cit.

to assist him or her in making a decision (which might be appropriate), and the Minister leaving the decision entirely to the computer programme.

6.8 Justice Perry doubts whether an administrative decision requiring the exercise of discretion or the making of an evaluative judgement requiring the balancing of different factors can be determined by an automated system, saying that "not only would there be a constructive failure to exercise the discretion" if automated systems were used in such cases, but the system would effectively be applying "predetermined outcomes which may be characterised as pre-judgment or bias."[27] Similarly Coglianese and Lehr note that 'significant regulatory policy decisions present complexities, uncertainties, and value judgments that will resist the kind of specification needed to embed them in mathematical objective functions.'[28]

6.9 For a decision that requires a human judgment and/or a right to a hearing to be left to a computer programme in our view arguably amounts to a dereliction of duty and an ultra vires attempt to delegate a discretion, because surely a discretion can only be delegated to a human being themselves capable of exercising real and genuine consideration of an issue (*Fay v Moramba Services Pty Ltd* [2010] NSWSC 725 at [34]–[40]; *Re Baden's Deed Trusts; McPhail v Doulton* [1971] AC 424 at 449; [1970] 2 All ER 228 at 240) with 'a fair consideration of the subject' (*Re Beloved Wilkes's Charity* (1851) 42 ER 330). **We are not convinced that the proposed delegation to a computer programme is either appropriate or legally correct and believe that the proposed section would result in a situation that arguably breaches Ministerial fiduciary duties.**

6.10 Section 56A is overbroad. It does not distinguish discretions from other decisions. Nor does it provide for a hearing in appropriate circumstances, or specify how a decision can be challenged in case of error. We submit that decisions made under this section have the potential to be found unlawful.

6.11 Section 56A does not appear to reflect Australia's own best practice Principles Nos 1 to 3 as set out in the *Automated Assistance in Administrative Decision-making: Better Practice Guide*,[29] itself based on the Administrative Review Council's *Automated Assistance in Administrative Decision-Making Report No. 46* to the Attorney General of 2004.[30] The principles state that:

- Automated systems that make a decision – as opposed to helping a decision-maker make a decision – would generally be suitable only for decisions involving non- discretionary elements.
- Automated systems should not automate the exercise of discretion.
- Automated systems can be used as an administrative tool to assist an officer in exercising his or her discretion. In these cases, the systems should be designed so that they do not fetter the decision-maker in the exercise of his or her power by recommending or guiding the decision-maker to a particular outcome. [31]

---

27 Ibid. See for example: NADH of 2001 v Minister for Immigration and Multicultural and Indigenous Affairs (2004) 214 ALR 264.

28 Cary Coglianese and David Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, (2017) 105 Georgetown Law Journal 1147 at 1214 available at: http://scholarship.law.upenn.edu/faculty_scholarship/1734/

29 Australian Government, *Automated Assistance in Administrative Decision-making: Better Practice Guide*, 2007, available at: https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf

30 Available at: https://www.arc.ag.gov.au/Documents/AAADMreportPDF.pdf

31 Andrew Le Sueur, "Robot Government: Automated Decision-Making and its Implications for Parliament", draft chapter in *A Horne and A Le Sueur (ed), Parliament: Legislation and Accountability, (Oxford, Hart Publishing, 2016),* 1 at 14 *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2668201,

6.12 Le Sueur suggests that automated decision-making systems should at the very least be required to provide explanations for their outcomes. Challenging a decision will be particularly difficult if no reasons are given for the decision. If explanations are required, this will support the element of the rule of law whereby procedures must be provided for citizens to resolve disputes with government without undue delay or cost.[32]

6.13 Dominique Hogan-Doran SC recommends that automated decision- making only be permitted where the automated system is built with proper verification and audit mechanisms so they can be reviewed by Ombudsmen, merits reviewers and judicial reviewers. She also recommends that code-makers be required to annotate the code to reference the relevant source material, such as statutes and policy. Without such requirements there can be no certainty, she says, that any automated decision-making system is lawful, transparent and fair.

6.14 As Katie Miller notes:

> The doctrine of the separation of powers means that it is for the courts, and not the executive, to determine whether a decision has been lawfully made. An assertion by the executive that the decision was lawfully made will not make it so.
>
> Applying this reasoning to technology-assisted decision-making, it is not enough for the executive to claim that it is using, or will use, technology in a way that promotes lawful decisions. There must be information available upon which the courts, integrity bodies and the public can assess this question for themselves. Put another way: you may say that technology has assisted you to make a lawful decision, but how do I know that? [33]

7. Conclusion

7.1 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 Bills do not strike the right balance.

7.2 ALHR is concerned that the Bills will severely impact on the privacy and other human rights of Australian individuals and is particularly concerned about the use of biometric data for commercial purposes and the attempts to divorce Ministerial decision-making from human control.

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 [redacted]

Yours faithfully

Kerry Weste

Acting President

Australian Lawyers for Human Rights

---

citing Australian Government, *Automated Assistance in Administrative Decision-making: Better Practice Guide*, 2007, Appendix B

32 Le Sueur, op cit at 9.

33 Katie Miller, "The Application of Administrative Principles to Technology-as-Decision-Making", (2016) 86 *AIAL Forum* 20 at 25, http://www7.austlii.edu.au/au/journals/AIAdminLawF/2016/26.pdf