Human Rights Law Centre

The dangers of unregulated biometrics use

Submission to the Inquiry into the *Identity-matching Services Bill 2018* and the *Australian Passports Amendment (Identity-matching Services) Bill 2018*

29 May 2018

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Prepared by

Dr Aruna Sathanapally (Director), Hannah Ryan (Lawyer), Angela Chen (Secondee Lawyer)

Human Rights Law Centre Ltd
Level 5, 175 Liverpool St
Sydney NSW 2000

T: + 61 2 8599 2128
E: hannah.ryan@hrlc.org.au
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas.

It is an independent and not-for-profit organisation and donations are tax-deductible.

Follow us at http://twitter.com/rightsagenda
Join us at www.facebook.com/HumanRightsLawCentreHRLC/

Introduction

1. The Human Rights Law Centre (**HRLC**) welcomes the opportunity to participate in the Committee's inquiry on the *Identity-matching Services Bill 2018* (**the Bill**) and the *Australian Passports Amendment (Identity-matching Services) Bill 2018*. We are grateful to the Committee for accepting this late submission.

2. We welcome the approach of providing a legislative framework for the retention, use and sharing of facial images and other biometric data. As we explain in this submission, new capabilities for search and surveillance must be law governed, and existing laws are insufficient to ensure this. **However, we have concluded that the proposed Bill is manifestly, and dangerously, insufficient for this purpose**.

3. This inquiry has benefitted from a small number of careful submissions which sound a clear warning bell about the system of powers and processes to be authorised by the two bills before the Committee. The HRLC shares these concerns, a number of which have been well articulated by others – noting in particular, the Australian Human Rights Commission, FutureWise and the Australian Privacy Foundation and the Law Council.

4. The most salient of these concerns are:

   (a) the very substantial erosion of privacy that would accompany upscaling government capacity to link and share personal information in the ways permitted by the two bills, including the manner in which the proposed regime would side-step privacy protections available in federal and state law;

   (b) the breadth of purposes – and entities – that the proposed regime would permit as a lawful foundation for use and sharing of biometric information, encompassing uses for which one may readily understand the need to limit privacy as well as other uses that appear far less pressing;

   (c) the distinct lack of evidence as to the need for such a broad and permissive regime; and

   (d) the absence of detail as to how the government in fact proposes to regulate the capabilities for which it seeks parliamentary approval.

5. Rather than engage in a comprehensive analysis of the Bill, which is made especially difficult by the absence of detail contained within it, we seek to make four targeted submissions.

6. The first (**Part 1**) is to draw the Committee's attention to the range of different risks created by different facial recognition capabilities, as set out by international experts (the Georgetown framework). This Bill fails to adequately identify or regulate these different potential uses, thereby constituting **a very high risk proposed regime**.

7. Next, we highlight particular concerns that the legislation must address *in addition to* privacy, being:

   (a) the impact on democratic freedoms of expression, association and assembly (**Part 2**); and

   (b) the discriminatory impact of algorithmic bias, that is, the greater incidence of false positives and false negatives in relation to individuals of particular minority ethnicities (**Part 3**).

8. Finally, we set out some parameters for how this type of technology ought to be broadly governed as it develops (**Part 4**). 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.

9. **New technological capabilities can and should flourish within our democratic processes of law and oversight, and we must ensure that they develop within the principles of a free society.** This Committee is a vital component of our parliamentary democracy: it acts as the principal vehicle through which our elected representatives contend with challenges to our national security and the difficult trade-offs in devising appropriate responses. A clear-eyed, long-term approach is essential for working out how to govern new and remarkable uses of biometric data that governments and others will enthusiastically develop and seek to expand. We would be pleased to assist the Committee further to identify the best path forward.

Recommendations:

1. **That the Bill be amended to include the substantive details of the contemplated regulation of the Interoperability Hub, the NDLFRS and the identity-matching services, so as to allow for a proper, informed parliamentary and public debate over the government's proposals.**
2. **That the purposes for which dragnet facial recognition searches or use of dragnet databases may be authorised be carefully constrained to investigation of serious criminal offences.**
3. **That any capability allowing real time surveillance be set out in proposed primary legislation to allow for a full assessment of whether its use is justified and safeguards are sufficient.**
4. **That the Bill not pass without safeguards to protect freedom of expression and other democratic freedoms in either the primary legislation, regulations or publicly available agency-level guidelines.**
5. **That the Bill include a requirement for annual accuracy testing based on demographics with results to be provided in annual reports.**

1. Understanding emerging biometric data capabilities

1.1 Facial recognition technology

10. Biometric data is data that relates to the human body and its measurements and features. Facial recognition is a type of biometrics tool. Broadly, facial recognition technology works by comparing an image of a face with another image of a face:

- **Facial identification** (or one-to-many matching) works by comparing the inputted image with a database containing a set of facial images. By reference to features of the face (like the width of the eyes and other physical features), the facial recognition service will then search for a match within the database.
- **Facial verification** (or one-to-one matching) compares the inputted image with only the image(s) held in relation to one person. In both cases, the matching process works on probabilities, with an algorithm calculating how likely it is that the person in the inputted image is the same person as that depicted in the potential match.

11. Facial identification systems may produce a shortlist of potential matches, with the user able to determine how many potential matches they wish to receive (and what degree of probability is sufficient to return a potential match). Facial verification systems will only compare the two images side-by-side and determine the probability that the people depicted in them are the same, based on the how the system has been 'taught' to identify likeness.

12. There are many potential uses for facial recognition technology. Many Australians will be accustomed to having their faces scanned as they re-enter Australia after a trip abroad: the "SmartGates" in our airports use technology to check that the person seeking to enter the country is the same depicted on the passport they are using without human intervention.

13. Facial recognition can also be used by law enforcement and intelligence agencies to locate, identify or track persons of interest or potential criminals. However, facial recognition technologies are **meaningfully different** from tools that law enforcement and intelligence agencies have previously had at their grasp. Unlike other tools which track technology such as mobile phones or cars, face recognition tracks a person's body.[1] A person's face is an enduring biometric indicator, for most people, it lasts a lifetime and is almost always on display. Paired with surveillance, it allows for tracking a person in a way that other biometrics which we are

[1] Clare Garvie, Alvaro M. Bedoya and Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America* (October 18, 2016, available at https://www.perpetuallineup.org/report) (**Georgetown Report**), 9-10.

more used to, like fingerprints, do not, as it allows for ongoing tracking, from a distance. According to a leading U.S. scholar:

> "Facial recognition represents the first of a series of next generation biometrics, such as hand geometry, iris, vascular patterns, hormones, and gait, which, when paired with surveillance of public space, give rise to unique and novel questions of law and policy. These constitute what can be considered Remote Biometric Identification (RBI). That is, they give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner. As such, RBI technologies present capabilities significantly different from that which the government has held at any point in U.S. history."[2]

14. Enabling and authorising the use of this kind of novel technology must therefore be carefully considered.

1.2 The Georgetown framework

15. In 2016, scholars from Georgetown Law's Center on Privacy and Technology published a landmark report examined the use of facial recognition by U.S. law enforcement agencies: *The Perpetual Line-up: Unregulated Police Face Recognition in America* (**the Georgetown Report**).[3] This report develops a useful framework to help identify the risk created by different categories of law enforcement uses of face recognition (**the Georgetown framework**).[4]

16. The Georgetown framework considers **five risk factors**, which in different combinations create different types of risks, and need different regulatory approaches. These factors are:[5]

Risk factor 1	**Targeted versus dragnet searches**	"Are searches run on a discrete, targeted basis for individuals suspected of a crime? Or are they continuous, generalised searches on groups of people …"
Risk factor 2	**Targeted versus dragnet database**	Is the database of images comprised only of known criminals or a watchlist, for example, or does it contain as many images as possible, including innocent people?
Risk factor 3	**Transparent versus invisible searches**	Do the people whose information is being searched for or retrieved know that the

[2] Laura K. Donohue, "Technological Leap, Statutory Gap, and the Constitutional Abyss: Remote Biometric Identification Comes of Age" (2012) 97 *Minnesota Law Review* 407, 415.

[3] Clare Garvie, Alvaro M. Bedoya and Jonathan Frankle, *The Perpetual Line-up: Unregulated Police Face Recognition in America* (October 18, 2016, available at https://www.perpetuallineup.org/report) .

[4] Georgetown Report, 16-22.

[5] Georgetown Report, 16-17.

		search has been carried out? ("*You can't challenge a search that you don't know about.*")
Risk factor 4	**Real-time versus after-the-fact searches**	Does the search aim to identify or locate someone right now (i.e. real time tracking)? Or is it run to investigate a person's past behaviour?
Risk factor 5	**Established versus novel use**	"Is a face recognition search generally analogous to longstanding fingerprinting practices or modern DNA analysis? Or is it unprecedented?"

17. On the basis of the Georgetown framework, it is possible to identify the spectrum of risks posed by different deployments of facial recognition technologies. For instance, a search targeted to a particular person of interest, based on a database of facial images of those with criminal convictions or current criminal charges, is at the **lower end of this spectrum**.

18. On the other hand, real-time video surveillance, based on a dragnet search across a database of images including innocent people, in a manner which is not known to those whose information is searched through and retrieved, poses **a very high risk** to fundamental rights including privacy and freedom of expression, association and assembly.

19. In light of the range of different risks to civil liberties posed by different uses and processes of facial recognition technology, legal regulation must be sensitive to these different risk factors. While certain uses of facial recognition may be analogous to existing law enforcement practices in Australia, **other uses depart dramatically from the level of surveillance that has been undertaken in liberal democracies**. These more dangerous uses must be subject to effective governance and oversight – including genuine public engagement over their place in Australian society and our meaningful consent to government's use of them – as they develop.

1.3 The proposed scheme carries a high risk rating

20. In October 2017, the Council of Australian Governments concluded the "Intergovernmental Agreement on Identity Matching Services" (**IGA**). Pursuant to the IGA, the states and territories agreed to share the images produced for their residents' driver licences, among other identification documents, to the federal government, so that they can be accessed by all jurisdictions via the "Interoperability Hub", a platform by which relevant agencies can access and share identity and biometric information. This information is retained in a centralised

database, the National Driver Licence Facial Recognition Solution (**NDLFRS**) which also consists of the identity-matching system.

21. The Bill is said to implement the IGA. The Bill provides the explicit legal basis for the Secretary of the Department of Home Affairs to develop and operate the Interoperability Hub and the NDLFRS, and to collect, use and disclose information to provide identity-matching services.

22. The Bill represents a significant step forward towards a new kind of society, different from the type of democracy we all understand Australia to be. Taken together, the IGA and the Bill allow for the creation of a centralised database and service, accessible by powerful agencies in the federal government, the states and the territories, containing the images of millions of innocent Australians. Facial recognition technology could mean that most Australians are involuntarily roped into participating in what the Georgetown Report authors have dubbed a '**perpetual line-up'**, where they risk being identified as a person of interest or criminal suspect and subjected to the potential of real-time surveillance that monitors their movements. **It is not just the technology described above that is relevantly novel, but also the centralised, coordinated nature of the Interoperability Hub.**

23. Insofar as the Bill represents an attempt to bring the development of new biometric capabilities into the framework of primary legislation, this is a vital task. **Our difficulty with the Bill is the nature of the framework it proposes, which is fundamentally not fit-for-purpose.**

24. The risk framework set out above illustrates why this is so, in relatively simple terms. The Bill would authorise and facilitate uses – by federal and State government agencies but also private businesses or local councils – that pose the highest risks to fundamental rights and freedoms:

    (a) The capabilities supported by the Bill include dragnet searches, with no proscription or limitation on searching for particular groups of people and no warrant system before a search is authorised.

    (b) The database is a **dragnet** – this will not be a database of mug shots or a smaller watchlist, but rather a database full of images of innocent Australians linked to personal information about each person, gathered from a variety of sources.

    (c) There is no requirement of **transparency** when searches are made. A person whose information is the subject of a search or retrieval will ordinarily not be made aware of this.

    (d) The Bill is silent on real-time versus after-the-fact searches, meaning it would allow real-time surveillance.

    (e) The Bill would allow for uses which are entirely novel.

25. Instead of setting out regulation that accounts for these different dimensions of risk – and instituting processes of authorisation and oversight commensurate with the risks that certain activities create, or may create as technology develops **– the Bill provides a broad and permissive authorisation for all of these activities to be undertaken as the database, and biometric data capabilities, develop**.

1.4 The proposed regime sidesteps existing privacy safeguards for biometric data

26. Given the ability to track a person's body, the collection, use and disclosure of biometric data should be subject to the individual's properly informed and voluntary consent. Biometric data is subject to more stringent requirements as a type of "sensitive information" under the *Privacy Act 1988*.[6] **Ordinarily, the *Australian Privacy Principles* (APP) would require individuals to consent to the collection, use and disclosure of this sensitive information.**

27. As raised in multiple other submissions[7], the Bill falls short when considered in light of the APP requirements on express or implied consent.[8]

(a) *The individual is **adequately informed before giving consent**.* This requires information about what is being collected, the proposed use and disclosure and consequences of failing to consent. As such, there should be an accessible and comprehensible explanation of the *identity-matching services* under the Bill and its interaction with obtaining other government services such as obtaining passports and drivers licences.

(b) *The individual gives consent **voluntarily**.* From the outset, the Bill does not allow individuals who obtain the relevant identification documents to withhold consent or opt-out of the facial recognition scheme. Without documents such as passports, driver licences and proof of age cards, individuals are limited in their ability to participate fully in society and move freely. As such, mere notification[9] does not provide alternatives and there are serious consequences for failing to consent.

(c) *The consent is **current and specific**.* Consent should not be broader than necessary for its immediate purposes and cannot be assumed for all future uses. Where there is a

[6] *Privacy Act 1988,* s 6.

[7] Submissions to the Inquiry into the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 by the Australian Human Rights Commission and the Law Council.

[8] Office of the Australian Information Commissioner, *Key Concepts Paper*, Version 1.2, March 2015. Note, we have not considered here the fourth element of *capacity* to consent.

[9] As proposed in IGA [6.19].

secondary purpose for the consent, the individual must be adequately informed of its usage. Individuals should also have the opportunity to withdraw consent.

28. For people who currently hold valid driver licences, it cannot be said that they provided proper informed consent for their photo to be now included in the national database. In the future, consent still is not easily discernible: the Bill raises the issue of "bundled consent" which traverses these three elements of consent. It is not apparent that when individuals provide free, informed and express consent to their photo being taken for a drivers licence they are also providing free, informed and express consent to the Australian Taxation Office to search and obtain their photo when applying for an ABN at indeterminate point in the future.[10]

29. However, the requirement of individual consent under the APP can be side-stepped where the collection, use or disclosure of the biometric information is required and authorised in law.[11] This is what the Bill seeks to do.[12] Likewise, state-level privacy protections contain carve-outs where federal law authorises use or disclosure, and the Bill expressly enlivens those carve-outs.[13]

30. **It is imperative that legislation that seeks to substitute the consent of individuals with the authorisation of Parliament is only passed after informed debate and careful scrutiny to ensure that it is targeted and fully justified.** There must be meaningful public consent to individuals' personal and sensitive information being used and shared by government agencies through the Interoperability Hub and the NDLFRS, given that use, overwhelmingly, will not have been individually consented to.[14]

31. Several submitters have provided valuable comment on the proportionality of the impact on privacy proposed in the Bill, and we do seek to repeat that analysis here. We would only add that, first, **"efficiency" alone is poor reason to justify uses of sensitive personal information that have not been consented to**. This has been recognised by the Council of Europe and the Australian Law Reform Commission specifically in the context of biometrics.[15] Therefore, assertions that facial recognition would more rapidly return results are only persuasive where time is of the essence and the objective is sufficiently serious. This cannot be the case in very routine and ordinary applications of the identity-matching services.

---

[10] See new section 18; Explanatory Memorandum [141] and [154].

[11] APP 3.4(a) and 6.2(b).

[12] See new sections 17 and 18 of the Bill.

[13] See new section 19 of the Bill.

[14] See below part 4.2.

[15] Council of Europe, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (2005), [107] at FN [154] cited in the Australian Law Reform Commission Report 108, *For Your Information: Australian Privacy Law and Practice*, 2008, [9.72].

32. Second, the European Court of Human Rights unanimously held in two separate instances (in relation to finger prints and DNA[16] and photographs[17]) that the retention of the biometric data of innocent persons in the database without consent or legitimate grounds disproportionately limited the right to privacy. This is reflected by recent developments in privacy law regarding when governments can deal with biometric data without consent. The European Union's *General Data Protection Regulation* which came into effect on 25 May 2018 recognises biometric data as a "special category of personal data" which can only be handled in limited circumstances, including "substantial public interest" so long as the measure is "proportionate to the aim pursued" and that there are "suitable and specific safeguards fundamental rights and the interests" of the individual.[18]

2. The use of facial recognition technology risks undermining freedom of expression

33. The threat biometric services pose to privacy has been well canvassed in other submissions (see submissions of FutureWise and the Australian Privacy Foundation and the Australian Human Rights Commission). Such technologies **also pose 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.

34. These freedoms are fundamental to Australian democracy. They are protected under international law, and political communication is protected under our Constitution.

35. Facial recognition technology, particularly real-time facial recognition, risks transforming public space into a sphere where each person can be monitored and identified. This is particularly concerning in the context of civic gatherings, demonstrations and protests. These are fundamental processes of democratic participation. There are many legitimate reasons why people may wish to add their voice to a cause without being personally subject to identification and monitoring. Those attending a public meeting or a vigil for instance should not have to have their identities revealed in order to exercise their democratic rights.

36. The risk facial recognition technology poses to freedom of expression has been explicitly acknowledged internationally, including by the U.S.' Federal Bureau of Investigation and the

[16] *S v United Kingdom* (European Court of Human Rights ,Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008).

[17] *Reklos and Davourlis v Greece* (European Court of Human Rights, First Section, Application no 1234/05, 15 January 2009).

[18] European Parliament and Council, General Data Protection Regulation, 2016/679, Article 9 and Recital 51.

Department of Homeland Security.[19] A Privacy Impact Assessment in which both agencies participated considered that:

> "The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behaviour, and lead to self-censorship and inhibition. These potential consequences of routine surveillance are often referred to as 'chilling effects.' … the risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance."[20]

37. Even if they have done nothing wrong, a person may not wish to attend a rally protesting against Aboriginal deaths in custody or police violence (as was recently at issue in Victoria), for example, when they know that police may be monitoring the rally and can near instantly identify them as a participant. The potential impact of facial recognition technology on freedom of expression is increased when protesters are forbidden or dissuaded from hiding their faces, as in Victoria.[21]

38. In addition to the principled position that Australians are entitled to have their say without identifying themselves, the use of facial recognition technology on public gatherings such as protests poses practical concerns. In a context where the technology is imperfect, false positives are an ever-present risk. Where facial recognition is used at a protest, protesters are then exposed to the risk that they will be detained, questioned, asked for identification, or any of the consequences of being wrongly identified as a person of interest to law enforcement agencies. This kind of consequence both prevents participants who are wrongly identified from fully participating in a protest, and deters those who would rather not be exposed to such a risk from participating in protests. In both cases, freedom of expression is compromised.

39. In other jurisdictions, law enforcement has used facial recognition technology to identify participants in protests and public events. For example, in March 2018, South Wales Police used automated facial recognition at a demonstration taking place outside an arms fair.[22]

40. When law enforcement has access to real-time facial recognition technology, there is also a risk of politically motivated surveillance. Historically, governments have used law enforcement agencies to monitor their political opponents or civil society leaders. Recently, U.S. law enforcement has conducted surveillance of Black Lives Matter protests and other

[19] The International Justice and Public Safety Network, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (30 June 2011), available at https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (**PIA**).

[20] Ibid 17.

[21] *Crimes Legislation Amendment (Public Order) Act* 2017 (Vic).

[22] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), available at https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf (**Face Off Report**), 15, 31. For other examples, including the targeting of individuals with mental health issues without consideration of the impact of biometric surveillance itself on mental health of vulnerable individuals, see Face Off Report 27-28.

demonstrations against police use of force.[23] This kind of surveillance is rendered more problematic when law enforcement are able to use the surveillance footage to identify each participant. Extensive surveillance paired with real-time facial recognition technology could allow law enforcement and intelligence agencies to track the movements of those whose opinions are uncomfortable or inconvenient.

41. We do not suggest that such politically motivated surveillance is a likely near-term consequence of this legislation. Rather, we draw attention to it because these are the types of possibilities that must be guarded against in the design of this system. In even the finest system of government, there may arise strong incentives for particular individuals to abuse powers, or for the exercise of powers to creep into new domains over time. It is for Parliament to best ensure that we do not enable these abuses, particularly as they may be difficult to detect as they happen.

42. Other jurisdictions have regulated their use of facial recognition technology to accommodate the particularly pressing interest in freedom of expression. For example, Ohio's rule on face recognition states:

> "Law enforcement may not employ this technology to conduct dragnet screening of individuals, nor should it use it to facilitate mass surveillance of places, groups or activities unless doing so further an official law enforcement activity. For example, it would not be appropriate for law enforcement to use facial recognition technology to conduct surveillance of persons or groups based solely on their religious, political or other constitutionally protected activities or affiliations unless doing so further an official law enforcement activity."[24]

43. **The Bill does not make any accommodation for protecting expressive activities or democratic freedoms.**

44. In light of the fundamental importance of freedoms of expression, association and assembly to Australian democracy, the impact of biometrics use on those freedoms must be taken into consideration when a law of this kind is contemplated. It is appropriate that the regulation of law enforcement and others' use of facial recognition and similar technologies make provision for this impact, and include measures to restrict the burden on democratic freedoms.

45. The Georgetown Report describes best practice as expressly addressing and enumerating activities that may chill freedom of expression. Specifically, the Georgetown Report

[23] Georgetown Report 42, see also for example George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson", *The Intercept* (25 July 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; George Joseph and Murtaza Hussain, "FBI Tracked an Activist Involved with Black Lives Matter as They Travelled Across the U.S., Documents Show", *The Intercept* (20 March 2018), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/

[24] Georgetown Report 44-45; Ohio Law Enforcement Gateway's Rules and Regulations, Rule 1.11, available at http://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf.

recommends an "express statement in a face recognition use policy prohibiting the use of face recognition to target or collect information on individuals on the basis of their race, religion, or other bases that may stifle speech."[25] A Privacy Impact Assessment drafted in 2011 by federal and state law enforcement agencies in the United States encouraged law enforcement policies around facial recognition to include provisions "concerning the appropriate use of a facial recognition field identification tool in areas known to reflect an individual's political, religious or social views, associations, or activities",[26] and that in such circumstances "the collection of long range lens photographs should be limited to instances directly related to criminal conduct or activity."[27]

46. Given the importance of these freedoms, and the absence of their effective protection in any constitutional or legislative charter of rights, we encourage Parliament to consider express protections in primary legislation. Even if it were decided that protections be included in regulations, or agency-level policy documents rather than in the primary legislation, that primary legislation should not be passed with these regulations or policies being devised and known to Parliament and the public. The Bill should only allow the country's law enforcement and intelligence agencies access to the Interoperability Hub and the vast database of images it contains with such regulations or policies being implemented by the relevant agencies.

47. We note that the Bill does refer to political opinions, and a range of other information as being excluded from the definition of "identification information" in s 5.[28] This serves to prevent information about political opinions from being shared, like facial images, through the Interoperability Hub. As the Explanatory Memorandum explains, the subclause makes it clear that the Bill does not "authorise Home Affairs to collect, use or disclose these types of information in the course of providing identity-matching services…. This is because these types of information are not needed to support the provision of the identity-matching services."[29] **But that does nothing to address the possibility that facial recognition technology, facilitated by the Bill, will be used in connection with expressive activities, such as to identify people attending a particular protest, raising the concerns set out above.**

[25] Georgetown Report 45.

[26] PIA 19.

[27] PIA 3.

[28] Section 5(2)

[29] Explanatory Memorandum 14.

3. Facial recognition technology imposes a disproportionate burden on people belonging to a minority ethnic groups

48. Any use of facial recognition technology must account for the accuracy and reliability of the results that it produces. Misidentification may have serious consequences, which must be accounted for when deciding any official uses for facial recognition technology, and the reliance placed on facial identification or verification results.

49. In particular, the burden that the use of facial technology places on rights, including but not limited to privacy, is amplified where the technology produces **false positives.** Where a false positive result is returned, a person suffers all the consequences of being identified as a suspect or person of interest – which may be further investigation, potential surveillance, the denial of a service, or the denial of employment – with no justification. This result is obviously concerning on its own. It is even more concerning where there are particularly groups who bear a greater risk of false positive associations.

50. **False negatives**, where a verification process fails because the technology does not identify a correct match, may also cause significant harm, depending on the decisions for which facial verification is used. For instance, the harm is lessened if there is a readily available secondary check. The harm is magnified where there is a significant administrative hurdle – or delay – caused by technological inaccuracy. This is particularly concerning where such errors occur in the visa and border control context, or in the context of the provision of essential services.

51. **Each of these dangers – false positive and false negatives – are likely to arise disproportionately in relation to people who belong to ethnic minorities in Australia.**

52. In a 2011 study conducted by the National Institute of Standards and Technology (**NIST**), the US Department of Commerce body which sets standards for facial recognition technology, it was found that facial recognition technology contains a bias towards the dominant ethnic group in the area in which it is developed. Facial recognition technology developed in East Asia was more accurate at identifying East Asian faces, whereas technology developed in Western countries was better at identifying Caucasian faces.[30] More recently, a 2018 study found that the misidentification rate for "darker-skinned" women was **34.7%** compared to 0.8% in relation to "lighter-skinned" men.[31]

[30] P Jonathon Phillips et al, "An other-race effect for facial recognition algorithms" *ACM Transactions on Applied Perceptions (TAP)*, 2011, 8(2):14.

[31] Joy Buolamwini and Timnit Gebru, 2018, "Gender Shares: Intersection Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research*, 81:1-15.

53. In operation, facial recognition technology has yielded even worse results. London's Metropolitan Police first used automated facial recognition at Notting Hill Carnival 2016, which is a celebration of London's Caribbean communities. It was also used at the same festival in 2017. In their Face Off Report, Big Brother Watch published information obtained via freedom of information requests to Metropolitan Police revealing that **over 98% of 'matches' wrongly identified innocent members of the public in their use of facial recognition systems**. Only two people were correctly identified using the technology; neither of whom was a wanted criminal. Overall, they discovered over 102 false-positive 'matches' in the course of the system's trial, the majority of which were attributed as attendees of Notting Hill Carnival.[32]

54. Such algorithmic bias can arise for various reasons, and given that source codes of leading face recognition software are not openly available it is difficult to identify the reasons with precision. What is known is that human software engineers develop the algorithm. To test and check its accuracy, they run the algorithm over sets of facial images. In more sophisticated technology, the algorithm may evolve based on usage, for instance, it will learn from human confirmation of a correct match, which fine tunes the algorithm.[33] As such, the algorithmic bias could reflect the "other race" bias whereby the human coders and persons regularly using the program (for instance, the police) find it difficult to discern distinctions between faces of persons of an ethnic background with which they are less familiar.[34] The accuracy of algorithms is also hampered where they are not tested against broad range of facial images from various demographics.[35]

55. Claims made by facial recognition technology providers and standards bodies (including NIST) should be treated with caution. Even NEC Neoface, the most accurate facial recognition as tested by NIST[36] which is used by federal bodies,[37] South Australian Police[38] and Northern

[32] Big Brother Watch, 25-26.

[33] Brendan Klare et al "Face Recognition Performance: Role of Demographic Information" *IEEE Transactions on Information Forensic and Security*, 2012,7(6):1789-1801. See also Georgetown Report, 53.

[34] P Jonathon Phillips et al, 2011.

[35] Brendan Klare et al., 2012.

[36] NEC, *NIST-proven accuracy*, <https://www.nec.com/en/global/solutions/safety/Technology/NIST_Proven_Accuracy/index.html?>.

[37] NEC, *CrimTrac selects NEC to provide national facial recognition and fingerprint matching capability* https://au.nec.com/en_AU/press/201605/crimtrac-nec-facial-recognition-fingerprint-matching-capability.html.

[38] NEC, *South Australia Police tap NEC for facial recognition edge over criminals*, <https://au.nec.com/en_AU/press/201607/south-australia-police-tap-nec-for-facial-recognition.html>.

Territory Police[39], has not been tested for accuracy based on demographics.[40] **As such, overall percentage accuracy results from NIST testing do not show accuracy on different ethnic groups and risk obscuring the disproportionately high rates of misidentification of ethnic minorities**.[41]

56. Moreover, accuracy is also subject to quality of the photos stored on and used to match against the database images (in this case, the images from the Interoperability Hub and NDLFRS). Exposure and lighting levels of images impact the ability of the technology to discern contours and map the face. The issue of bias emerges again as default settings on cameras in Western countries are usually programmed to identify faces of lighter skin tone.[42] **Therefore, even if code is advanced to the point whereby algorithmic bias is removed, the bias resulting from the quality of the images remains problematic.**

57. **Misidentification risks eroding trust in government agencies, law enforcement and security agencies**. This concern is exacerbated in the case of minority ethnic groups. As seen from the issues of racial profiling by police, this risks stoking tensions with communities who bear the brunt of mistakes and compromising effectiveness of policing.[43] The Georgetown Report draws attention to the impact of facial recognition in the United States on the rates of arrest of African American stating that "face recognition may be overused on the segment of the population on which it underperforms".[44] Big Brother Watch in the UK remarks on how "disproportionate misidentifications risk increasing the over-policing of ethnic minorities on the premise of technological "objectivity"".[45] In Australia, we should consider carefully how facial recognition technologies are likely to operate in our ethnically diverse society, in particular, the potential impact Aboriginal and Torres Strait Islanders who are overrepresented in arrest and incarceration rates.

---

[39] NEC, *NEC facial recognition helps NT Police solve cold cases and increase public safety in Australia* <https://au.nec.com/en_AU/press/201509/nec-facial-recognition-increases-public-safety-in-australia.html>.

[40] Big Brother Watch, 16; see also Mann and Smith, 2017.

[41] Buolamwini and Gebru, 2009. Note also, the 2018 study highlighted that the NIST dataset against which accuracy was tested had 79.2% "light skinned" faces, which further casts doubt on adequacy of the accuracy testing process.

[42] Lorna Roth "Looking at Shirley, the ultimate norm: Colour balance, image technologies, and cognitive equity", *Canadian Journal of communication*, 2009, 34(1):111, cited on page 4 of Buolamwini and Gebru, 2009.

[43] Victorian Police, *Equality is not the same*, http://www.police.vic.gov.au/content.asp?Document_ID=47751. This report was published after Community Consultation and Reviews on Field Contact Policy and Data Collection and Cross Cultural Training initiated after settlement of litigation in February 2013 regarding the use of racial profiling by police.

[44] Georgetown Report, 53.

[45] Big Brother Watch, 17.

4. The use of biometric data must be law-governed and the regime must have meaningful public consent

58. As demonstrated by these and other submissions to this inquiry, the use of biometric technology by governments is a vivid example of technology outpacing the law. Globally, the developing technology has been used by law enforcement and other government agencies in various countries without sufficient scrutiny and oversight.[46] This is also true of Australia, where facial recognition technology is used by our law enforcement bodies without any specific guiding legislation, and few safeguards.

59. This is not to say that biometric technology does not offer benefits for a variety of public policy objectives, including public safety. But the threats to fundamental rights of expression, privacy and freedom from discrimination are sufficiently serious as to require:

(a) Appropriate **legal regulation** which defines the permissible uses of the technology, and the circumstances in which those uses can be accessed (**i.e. there should be a legislative basis for governments to use facial recognition technology, which also includes appropriate safeguards**); and

(b) A robust, informed **public debate** about what that regulation looks like.

4.1 Facial recognition must be regulated by law, and that law must be sufficiently detailed

60. In broad terms, the Bill **facilitates, but does not genuinely regulate, the use of facial recognition by government bodies**. The Bill provides a permissive basis for the legality of facial recognition and facilitates its use in relation to a database accessible by every Australian jurisdiction. It lacks the detail required to properly ensure the proportionality of this technology's use in view of its impacts on fundamental democratic values. It is light on safeguards. For example, there is nothing in the Bill to limit the very highest risk uses of face recognition described in Section 2 above, except that if the request for facial identification comes through the Interoperability Hub, it must be made by an intelligence, law enforcement or integrity agency, for an "identity or community protection activity", broadly defined (for example, it includes investigating an offence but there is no seriousness requirement attaching to the offence). Within that broad class of agencies and activities, **the law prescribes no specific safeguards**.

[46] See, for example, the conclusions contained in the *Report of the Independent Advisory Group on the use of Biometric Data in Scotland* (March 2018, available at http://www.gov.scot/Publications/2018/03/9437) and the Georgetown Report.

61. Although the Bill regulates by broad strokes, even those broad strokes are subject to alteration by extra-parliamentary means. Under the Bill, the Minister may make rules,[47] including

    (a) To add to the categories of "identification information" that come within the Bill's purview;[48] and

    (b) Any rules that are "necessary or convenient" for carrying out or giving effect to the Bill.

    The Minister's rule-making power under this Bill should not be so broad or consequential. In this respect, the Centre adopts Recommendation 8 of the Australian Human Rights Commission's submission and the analysis at 6.4 and 6.5(f).

62. As to the safeguards the Bill includes, those are:

    (a) A prohibition on public servants recording or disclosing certain information from the NDLFRS, except for the purposes of the Bill (which are broadly drawn) or when exercising powers relating to the Interoperability Hub or the NDLFRS, or in certain other circumstances: Part 4.

    (b) The requirement to provide an annual report (which the Law Council notes does not include a requirement to report the details of non-government access to the FVS, and excludes material relating to ASIO);[49] and

    (c) A review of the Act and the provision no identity-matching services within five years of its commencement.

    Weighed against the novelty and riskiness of the kinds of technologies that the Bill facilitates government use of, these safeguards are wholly insufficient.

63. Without adequate legal regulation, critical decisions about how we treat Australian's privacy and freedom of expression, and the kind of democracy that Australia is, are left in the hands of Ministers and departmental officials with little in the way of constraints or oversight. **But these are exactly the kinds of significant decisions that the Parliament should be making.**

64. This is especially in Australia's legal context. Unlike other Western democracies, Australia cannot rely on the judiciary to provide a backstop on incursions to privacy and other rights when technology or government practice outpaces legislating. There are scarce tools like a Human Rights Act or constitutional protections that would allow them to do so. It is therefore imperative that Parliament be actively engaged in this type of legislation.

[47] Section 30.

[48] Section 5(1)(n).

[49] Section 28.

65. This submission does not attempt to comprehensively outline how facial recognition should be properly regulated. However, the following best practice principles can be distilled from resources such as the Georgetown Report – each of which are **not** encompassed in the Bill:[50]

(a) Laws which require law enforcement and domestic intelligence agencies to have a **reasonable suspicion of criminal conduct prior to a face recognition search**;

(b) After-the-fact investigative searches – which are invisible to the public – should be limited to **criminal offences of sufficient severity (such as indictable offences)**;

(c) Mug shots, not driver licence and identification photos, should be the default photo databases for face recognition for law enforcement and security purposes, and they should be periodically scrubbed to eliminate the innocent;

(d) Except for identity theft and fraud cases, **searches of licence and ID photos should require a court order** issued upon a showing of reasonable grounds to believe that a particular person has committed a crime, and should be restricted to serious crimes. The fact that these searches are allowed should be publicly available;

(e) **If real-time face recognition is allowed, "it should be used as a last resort** to intervene in only life-threatening emergencies. Orders allowing it should require probable cause, specify where continuous scanning will occur, and cap the length of time it may be used."[51]

66. **Other submissions to this Inquiry** identify features that the Commonwealth's regulation of facial recognition should bear, including (but not limited to):

(a) The core features of the design and operation of the Interoperability Hub, and the functionality of the identity-matching services, should be specified in the Bill's text (Australian Human Rights Commission, Recommendations 2 and 3);

(b) Warrant requirements for certain uses of identity-matching services (Australian Human Rights Commission, Recommendations 4 and 5);

(c) Provisions regarding the length of retention of identification information (Australian Human Rights Commission, Recommendation 6);

(d) Appropriate oversight (for example, Victorian Government submission at 1);

(e) Internal consistency of terminology (see Law Council of Australia, 8(a)); and

[50] Georgetown Report 4.

[51] Georgetown Report 4.

(f) Clarity regarding its interaction with the *Privacy Act 1988* (Cth) (see Law Council of Australia, 8(c)).

67. We support each of these submissions. Compared against the content of the Bill, they indicate that vital parameters and safeguards which should be included in any legislation of this kind, and which are not included in the proposed law.

4.2 This regulation must be informed by a robust and informed public debate

68. This kind of legislation cannot proceed without a robust and informed public debate. Biometric technologies hold great potential for transforming the nature of our society – and the ordinary person's anonymity in a range of common activities, and in a range of a democratic activities. Regulation of these novel technologies, and active facilitation and development of them for collective purposes, must be informed by an **educated public debate which has been to date almost entirely absent.** The type of enduring regime sought to be introduced by this Bill cannot proceed without the meaningful consent of the Australian people.

69. We therefore share the serious concerns voiced by many others about the process by which this Bill has proceeded. After an Intergovernmental Agreement was concluded by the executives (and therefore without appropriate democratic input), this Bill was introduced on 7 February. On 8 March, the Committee called for submissions to be on 21 March, with the report initially scheduled to be delivered in mid-May.

70. For example, it is critical **that the types of images that are retained should be the subject of public debate**. In other comparable jurisdictions, there is robust and ongoing discussion about whether it is appropriate that images of those taken into custody but who are innocent should be retained in a facial recognition database, and how long images should be retained for.[52] In Australia we have gone much further, making our database as broad it could possibly be by including all driver licences and passport/visa photos without that kind of debate.

71. The passage of the metadata retention legislation, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, is instructive here. It is analogous as an example of a time when a new technological capability was made available to law enforcement

[52] See Face Off 21-24; *Report of the Independent Advisory Group on the use of Biometric Data in Scotland* (March 2018, available at http://www.gov.scot/Publications/2018/03/9437) 9-10. See also decisions of the European Court of Human Rights like *S v United Kingdom* (European Court of Human Rights ,Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008), in which hit was held that the indefinite retention of biometric information after criminal proceedings resulting in no recorded conviction was "a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society" and above paragraph 32. See Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" (2017) 40 *University of New South Wales Law Journal* 121, 134-135.

on public safety grounds. The process leading to the Act's passage raised serious concerns, for example the quality of the public debate in the media,[53] and the swift abandonment of this Committee's inquiry into access to a journalist's source through metadata.[54] However, **even that process far out-stripped the present one in duration and level of engagement**. The Act's passage followed this Committee's 2012-2013 inquiry into potential reforms of Australia's national security, and a subsequent 2014-2015 inquiry into the Bill itself. The former inquiry lasted almost one year. The inquiries received 241 submissions and 204 submissions respectively. While the passage of that Act was rapid, by comparison this proposed progress of this Bill is even more radically compressed: with a proposed turnaround of two months in Committee, with the benefit of only 15 submissions at the date of writing.

5. Recommendations

72. For the reasons set out above, we r**ecommend that this Committee conclude that the Bill lacks sufficient detail** of the contemplated regulation of the Interoperability Hub, the NDLFRS and the identity-matching services, and **recommend that the Bill be amended to include this detail**, so as to allow for a proper, informed parliamentary and public debate over the government's proposals. Without this level of detail, it is virtually impossible to properly assess what the government is asking of Parliament and the Australian public.

73. In light of the high risk that these uses pose, we recommend that **the purposes for which dragnet facial recognition searches or use of dragnet databases may be authorised be carefully constrained to investigation of serious criminal offences**. Further, **any capability allowing real time surveillance must be set out in proposed primary legislation to allow for a full assessment of whether its use is justified and safeguards are sufficient**.

74. In addition to the recommendations made by others to protect privacy, we recommend that the **Bill not pass without safeguards to protect freedom of expression and other democratic freedoms in either the primary legislation, regulations or publicly available agency-level guidelines**. We also recommend that **the Bill include a requirement for annual accuracy testing based on demographics with results to be provided in annual reports**.

[53] See Laurie Oakes, "'These things can't just be left to government': Transcript of Laurie Oakes' remarks at Melbourne Press Freedom Dinner" (28 September 2015), available at http://www.walkleys.com/these-things-cant-just-be-left-to-government-transcript-of-laurie-oakes-remarks-at-melbourne-press-freedom-dinner/.

[54] See Parliamentary Joint Committee on Intelligence and Security, "Media Alert: Committee Concludes Inquiry Into Access to Journalists' Metadata" (8 April 2015), https://www.aph.gov.au/DocumentStore.ashx?id=721b078b-45b1-4746-871d-414e7f8be81b.