Australian Human Rights Commission

3 September 2019

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

By electronic submission

Dear Committee,

Review of the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019

The Australian Human Rights Commission (Commission) welcomes the opportunity to make this brief submission to the Parliamentary Joint Committee on Intelligence and Security (Committee) review of the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019 (the 2019 Bills).

We note that the terms of the 2019 Bills are the same as those of two Bills which were introduced in 2018 and lapsed prior to passage — the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (the 2018 Bills). The Committee commenced an inquiry into the 2018 Bills but did not report prior to the dissolution of the last Parliament.

As the Committee's webpage for this inquiry notes, the Committee has accepted as evidence in this review all evidence it received in its review of the 2018 Bills, including submissions and transcripts of hearings held in that inquiry.

The Commission provided a detailed submission to the Committee in March 2018 as part of its review of the 2018 Bills.

The Commission also gave evidence before the Committee at a public hearing on 3 May 2018, following which it made a supplementary submission responding to questions taken on notice at the hearing.

The Commission continues to hold serious concerns that the Bill would impinge on a number of human rights in ways not demonstrated to be necessary and proportionate to achieving its objectives. Rights that are particularly likely to be limited are the right to privacy, freedom of movement, the right to non-discrimination, and the right to a fair trial, though this is not an exhaustive list. The Commission refers to and repeats its written and oral submissions made in relation to the 2018 Bills, and the recommendations contained in them. Copies of the Commission's written submissions are attached for reference.

These Bills can operate only through heavy reliance on biometric facial recognition technology. This remains a relatively new area of technological development. In its submission on the 2018 Bills, the Commission drew particular attention to the fallibility of biometric facial recognition technology in practice and the potentially serious human rights implications of its use.[1]

We know that researchers and companies seeking to commercialise such technologies have made, and are continuing to make, significant progress in developing their capabilities. However, the leading academic research makes clear that the technology, generally, remains unreliable, particularly compared to humans' capacity to recognise faces, which is itself prone to error. This is particularly the case in 'real-world' applications, which generally involve the use of lower-quality images taken in sub-optimal conditions.

The proliferation in the use of this type of technology continues with increasing use in a law enforcement context. Since the Commission's submission on the 2018 Bills, research continues to lend weight to the Commission's concerns about the use of this technology, particularly in a law enforcement context.

The research casts serious and fundamental doubts about the reliability of biometric facial recognition technology in general. In this regard, the Commission refers the Committee to recent studies demonstrating the presence of bias emerging from biometric facial recognition technology in the identification of gender and race.[2]

The use of biometric facial recognition technology has been shown to be particularly unreliable when used in the identification of persons belonging to particular sections of the community. Market leading facial-recognition applications have been shown to be particularly unreliable when used on

headshot photographs of people with darker skin, women and people with a physical disability. This can disadvantage members of those groups in several ways. In the context of law enforcement, lower reliability increases the likelihood that innocent people will be misidentified and become subject to investigation or coercive action by law enforcement and intelligence agencies. In the case of service delivery, it may make it more difficult for members of those groups to establish their identity and to access services including government and financial services.

Australia must be vigilant to the threats that the use of this technology can pose to fundamental human rights. Some jurisdictions are being proactive. For example, in May 2019 San Francisco's board voted to ban the use of facial recognition technology in the city.[3] In July 2019, the UK's Information Commissioner's Office commenced an investigation into the use of facial recognition technology by law enforcement.[4] And in June 2019, the European Commission's *High-Level Expert Group on Artificial Intelligence* suggested the banning, or at least curbing, of some biometric technologies including facial recognition software, and that 'red lines' be set over the extent to which the technology can be used.[5]

In some other jurisdictions, trials of the technology continue. Yet the evaluation of such trials paint a worrying picture. For example, earlier this year an evaluation of the trialled use of one such facial recognition system — known as 'Neoface' — by the Metropolitan Police Service in a number of areas of London revealed that the overwhelming majority of 'matched individuals' were incorrectly identified.[6]

These evaluations reinforce the Commission's views, explained in its submission on the 2018 Bills, about the negative consequences that can flow from inaccurate biometric identifications, including in the law enforcement context.[7] The severity of these consequences, — particularly for the individual concerned, but also to the public at large — is difficult to predict and can vary widely according to the context in which the technology is employed.

The Commission has pointed to the risks that the use of such technology may have in restricting fundamental, and at times non-derogable, human rights such as the right to equality before the law and protection from discrimination.[8] If inaccurate information received from the use of this technology is used by law enforcement, it could also have drastic consequences for the person concerned, including being arbitrarily detained and having fundamental features of their right to a fair trial compromised.[9]

Similarly, the Commission warned in its submission on the 2018 Bills[10] that information about a person's age, race, sex, and health may be deduced from facial images creating an inherent risk that the technology could be exploited and used to profile persons on these bases. This gives scope for its use to routinely invoke the right to non-discrimination protected under article 26 of the *International Covenant on Civil and Political Rights*.

The Commission reiterates its principal recommendation that the Bill not be passed. We urge the Committee to consider closely all of our alternative recommendations should it be minded to recommend the Bill proceed.

The Commission remains at the Committee's disposal should it be able to assist further.

Edward Santow
Human Rights Commissioner

T +61 2 9284 9608
F +61 2 9284 9794
E humanrights.commissioner@humanrights.gov.au

---

[1] Australian Human Rights Commission, Submission: *Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018*, 29 March 2018, [14]-[32] (AHRC Submission to the 2018 Bills).
[2] See, for example, Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) *Proceedings of Machine Learning Research* 81(1) 1-15.
[3] Known as the *Stop Secret Surveillance Ordinance*.
[4] Elizabeth Denham (Information Commissioner), *Blog: Live facial recognition technology – data protection law applies* (9 July 2019), available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/blog-live-facial-recognition-technology-data-protection-law-applies/>.
[5] European Commission, Independent High-Level Expert Group on Artificial Intelligence, *Policy and Investment Recommendations for Trustworthy AI* (June 2019), available at <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60343>.
[6] See Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Face Recognition Technology', *The Human Rights, Big Data and Technology Project* (July 2019), available at <http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>.

[7] Generally, AHRC Submission to the 2018 Bills, [22]-[25].
[8] AHRC Submission to the 2018 Bills, [52]-[55].
[9] AHRC Submission to the 2018 Bills, [42].
[10] AHRC Submission to the 2018 Bills, [42].

Australian Human Rights Commission

Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018

AUSTRALIAN HUMAN RIGHTS COMMISSION SUBMISSION TO PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

29 March 2018

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Table of Contents

1 Introduction

1. The Australian Human Rights Commission (Commission) makes this submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in relation to its review of the Identity-matching Services Bill 2018 (Identity Bill) and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (Passports Bill). This submission focuses primarily on the Identity Bill.

2. The Commission is established by the *Australian Human Rights Commission Act 1986* (Cth) and is Australia's national human rights institution.

3. This submission addresses the potential impact of the Bills on human rights, and in particular the right to privacy. That right, enshrined in article 17 of the *International Covenant on Civil and Political Rights* (ICCPR),[1] may permissibly be limited by measures that are necessary and proportionate to achieve a legitimate aim, if protected by safeguards and oversight.

4. The Commission recommends that the Bills not be passed in their current form. In the event that recommendation is not accepted, the Commission makes a number of alternative recommendations designed to ameliorate the Bills' impact on human rights.

2 Recommendations

5. The Australian Human Rights Commission makes the following recommendations:

Recommendation 1

The Bill should not proceed in its current form.

Recommendation 2

If the Bill proceeds, it should be amended so that the core elements of the design and operation of the interoperability hub should be specified in the text of the Bill, rather than being left to the discretion of the Secretary.

Recommendation 3

If the Bill proceeds, the provisions defining each of the identity-matching services should be substantially redrafted, so that their functionality is fully defined in the Bill.

Recommendation 4

If the Bill proceeds, it should be amended so that access to the FIS is only available on the issue of a warrant.

Recommendation 5

If the FIS proceeds, it should be available only on the issue of a warrant.

Recommendation 6

If the Bill proceeds, it should be amended to ensure that any identification information disclosed in the response to a request for an identity-matching service is not retained beyond the time necessary to verify or establish identity.

Recommendation 7

If the Bill proceeds, it should be amended to ensure that identification information produced in response to a request for an identity-matching service is not used for any purpose other than establishing or verifying identity.

Recommendation 8

The Minister's rule-making powers in sections 5(1)(n) and 7(1)(f) of the Bill should not be passed.

Recommendation 9

If the Bill proceeds, the definition of 'identity or community protection activity' in section 6 should be amended so that:

- limb (a) of the definition of 'law enforcement activities' in subsection (3) includes only the prevention of *serious* offences
- subsections (7) and (8), dealing with 'road safety activities' and 'verifying identity' are deleted.

3 Background and Overview

6. In 1986, the Australian government introduced the Australia Card Bill 1986 in the House of Representatives. The objectives of that Bill included reducing tax evasion, welfare fraud and illegal immigration. It would have established a national identity card, as well as a central register of information relevant to that card.

> The scheme [was] based on large-scale computer matching. The [Health Insurance Commission, which would have maintained the central register] would [have been] permitted to expropriate and match data from a wide variety of sources, including 16 government agencies and the individual himself…. Moreover, the scheme [was] designed to facilitate, indeed automate, such activities in the future.[2]

7. The Bill attracted significant public scrutiny and was ultimately defeated in the Senate.[3]

8. The Identity Bill would not create a national identity document. It would, however, create a 'hub' linking a number of very large databases of personal information both of Australian citizens, and of non-citizens who have entered or sought to enter Australia. It would make the repositories of information that come within the scheme available for a number of purposes: to verify the authenticity of identification documents, to verify the identity of individuals, and

to identify unknown individuals. The services created by the Bill would primarily do this by making comparisons of biometric data — initially by use of face-matching technology. It is envisaged, however, that further biometrics might in future be used.

9. The principal object of the Identity Bill is stated to be 'to strengthen the integrity and security of Australia's identity infrastructure', and through this means, 'enhance national security, combat crime and increase service delivery opportunities.'[4] The Bill is also directed to a number of more or less closely related goals, for instance improving road safety, including by 'mak[ing] it harder for persons… to avoid traffic fines, demerit points or licence cancellations'.[5]

10. In some ways, the Bills could help protect the privacy or other human rights of individuals by providing them with enhanced security in relation to their own personal information. On the other hand, the Bills would impinge on the privacy of a large number of people by allowing their personal information to be collected, stored and shared. The Bill would allow this to be done in a number of ways and to serve a number of different objectives.

11. The Bills would primarily operate by allowing computerised comparisons to be made between facial images and other personal information for the purposes of verifying the authenticity of certain 'identity documents', verifying individuals' claimed identities, and identifying unknown individuals. While the Bill currently places an emphasis on facial images, the Minister could make rules, without the full parliamentary oversight involved in new primary legislation, to provide new services involving the comparison of any other biometric information. The comparison of biometric data is an essential component of the Bill, because, it is said, comparisons of purely biographic information cannot protect against the fraudulent use of that information by third parties. That is, biographic data can be stolen, and it is difficult to determine whether a person who claims it as their own is being truthful.[6]

12. The Commission has a number of concerns about the Bills. In particular:

    a. The Bills would allow personal information collected for particular purposes to be used for different purposes. In some cases, at least, this dramatically increases the impacts on the privacy of those from whom the information has been (and will be) collected. This is exacerbated by the fact that much of the information that will be made available under the Bills was (at least in some sense) provided voluntarily.

    b. The Bill is extremely broadly drafted. A great deal of detail about how key aspects of the Bill would operate is left to the discretion of a departmental secretary.

    c. At least some of the identity-matching services defined in the Bill could potentially allow for very intrusive surveillance to be conducted in public places. Some key limits on how the services would or would not be used are mentioned in the Explanatory Memorandum, but do not feature in the Bill.

d. The Minister would be given very broad powers to define new kinds of 'identity-matching services' and the kinds of information that could be shared through them. These powers could lead to further very significant intrusions on privacy.

e. Some of the purposes for which identity-matching services may be used do not appear to be of sufficient weight to justify potentially significant limitations on privacy. Others are so broadly defined that they might be interpreted to allow law enforcement bodies and intelligence agencies to use the services to collect information almost without limitation.

f. The Identity Bill places no limits on what may be done with information shared through the services the Bill would create.

g. All of the identity-matching services have at least some risk of returning false positives or false negatives. However, the services designed to identify unknown people will necessarily return a number of false positives every time they are used. These services are generally intended to be used by law enforcement and intelligence bodies. That means that innocent people will have their personal information shared every time those services are requested. They will also become persons of interest to the agencies that have requested the service.

h. It is far from clear that some of the objectives the Identity Bill is designed to achieve can justify the limits on privacy and other rights that the use of the identity-matching services could entail.

13. This submission contains:

a. A brief discussion of biometric technologies and the ways their use may engage the right to privacy

b. A discussion of the relevant international law concerning the right to privacy and its application to biometric identification technologies

c. A discussion of the operation of the identity-matching services that would be established by the Identity Bill

d. A discussion of the types of personal information that would be used and disclosed under the Identity Bill and the potential extent of that disclosure

e. A discussion of the ways the Identity Bill would limit the right to privacy

f. A number of recommendations.

4 Biometrics and biometric identification

14. The Identity Bill will establish various 'identity-matching' services. The Bill and the secondary materials make clear that these services will involve the use of biometric facial recognition technology. The Bill and secondary materials also

make clear that new forms of identity-matching services may be established (under Ministerial rule-making powers) using other biometric identifiers. The operation of the Bill is discussed later in this submission.

15. Biometric identification technologies, including facial recognition technology, are extremely powerful tools. They are particularly powerful, and particularly intrusive on privacy, when they are linked with other databases that contain personal information.[7] The following brief discussion is intended to provide some context for the discussion of the ways that the technology may intrude on privacy.

16. The Australian Law Reform Commission (ALRC) defined biometric systems as systems 'which enable unique behavioural or physiological attributes of people to be used for identification and authentication'.[8] The ALRC gave as examples of biometric technologies facial recognition, fingerprint scanning, iris and retinal scanning, finger geometry, voice recognition, dynamic signature verification, ear geometry, body odour measurement, keystroke dynamics, gait recognition, and palm vein recognition.[9] Other current or possible biometrics that are described in the literature include body scans,[10] DNA pattern analysis, sweat pore analysis, various patterns of movement, 'psychological' biometrics involving the measurement of responses 'to concrete situations or specific tests to conform to a psychological profile,[11] and measurement of electro-oculograms, electro-cardiograms, and electro-encephalograms (ie brainwaves).[12]

17. A former Privacy Commissioner has said that the number of biometrics that may be devised 'is probably limited only by our imaginations'.[13] The list of biometrics being developed continues to expand. It has been said of 'second generation', 'soft' biometrics in development that:

> The dream of [the] second generation of biometrics is a person's identification on the basis of that person's dynamic behaviour. In this respect second generation biometrics play a role in the wider field of behavioural surveillance. In fact, the attempt is not made to identify a person, no: the objective is to read the person's mind.[14]

18. There may be variation in the way biometric technologies operate. For instance, facial recognition systems can employ colour, black or white, or infrared, images; or two- or three-dimensional images.[15]

19. Biometric systems involve taking some sample — such as a photograph of a face — and 'enrolling' it, which is essentially preparing a template based on a series of measurements. Today this process is computerised.

20. Biometric systems rely on the fact that the features measured are unique (or virtually unique), in general do not change with time (though in some circumstances, such as through injury or through ageing, they may), and are not susceptible to being 'lost' or forgotten in the way other identity tokens may be.

21. Biometric systems may be used to verify claims of identity. They can also be used to identify an unknown person. In either case, the process involves obtaining a biometric sample and comparing it with a template held elsewhere.

22. Because biometrics are seen to be based on what are said to be unique characteristics, there is a risk that biometric identification may be perceived to be more accurate than may be the case. Biometric technology is inherently probabilistic. Its accuracy depends on a range of factors including the quality of the samples (eg photographs) used. As an expert group convened by the Council of Europe has observed in relation to biometric identification processes, 'any assumption of infallibility is erroneous.'[16] Choices must be made about how close a 'match' is required between two templates before the software employed reports a 'match'. Requiring an exceptionally close match will increase the rate of false negatives, or false rejections, returned by the system. Setting a less stringent requirement for a match will increase the rate of false positives, or false acceptances, returned by the system. Both of these consequences may have a negative impact on the individuals involved.

23. Where access to a service or a benefit is dependent on establishing identity, a false negative will preclude the person from accessing the service. That may interfere with a whole range of human rights, including civil and political as well as economic, social and cultural rights.

24. False positives may have even more serious consequences. For instance, where law enforcement or security persons are seeking to identify an unknown person, a false positive is likely to result in a person being identified as a suspect. They may be placed in a situation where, in practical effect, they are required to establish their innocence.

25. Where biometric systems are used to verify identity, they may simply return a response of 'match' or 'no match'. That limits the impact on privacy of an incorrect result. When, on the other hand, such systems are used to establish the identity of an unknown person, a false positive result can have very serious consequences for the person involved, particularly in the context of law enforcement.

26. Because biometric markers cannot, in general, be 'lost' or alienated from a person, biometric systems can also give an illusion of impregnable security.

27. It is true that biometric technology can be employed in ways that increases privacy and security. However, like all systems, biometric identification systems may be compromised. A wide range of techniques may be employed to circumvent biometric identification systems.[17] These include administrative abuses by persons with access to relevant systems, spoofing (for instance, making artificial fingers),[18] coercion of individuals to provide biometric samples (using force to make them place their finger on a scanner at an ATM, for example), and, according to one report, cutting off the finger of a target (in that case, to steal a car which used a biometric system to gain access).[19] They also include many computer-based techniques.

28. While statements may be found to the effect that a 'biometric cannot be reverse engineered',[20] advances in technology have led to that statement no longer being universally true. For instance, fingerprints have been successfully reconstructed from minutiae templates.[21]

29. Use of biometrics creates new risks. Unlike other methods for establishing identity, including knowledge-based systems (such as the use of passwords), a biometric identifier cannot be revoked or reissued. Once compromised, it can no longer be used. If a service provider requires a person to provide a particular biometric identifier to access a service, compromise of that biometric may place the affected person in an extremely difficult position. Further, where a particular biometric identifier is widely used, or is associated with large amounts of biographic data, theft or compromise of the biometric may facilitate access to, and the collation of, huge amounts of personal information about the target.

30. For these reasons, it has been argued that the use of biometric systems in fact increases the risk of identity fraud and theft.

31. 'Exposed biometrics', including facial recognition systems, can facilitate the surveillance and even tracking of individuals. In this way, biometric technology can, if its use is not carefully regulated, be extremely destructive of the right to privacy. The potential for biometric identification technologies to be used to conduct widespread surveillance, and tracking of individuals, is real. Some examples of current biometric identification technology include:

    a. linking CCTV cameras to biometric databases in real time. The resulting 'smart CCTV' allows the location of anyone in the relevant databases to be monitored, and their behaviour observed and recorded. Smart CCTV is already in use in the United Kingdom.[22]

    b. It has recently been reported that Chinese authorities have implemented a new surveillance system in Shenzen that is

        > … loaded with facial recognition, artificial intelligence, and a big database to crack down on jaywalking as well as other crimes.
        >
        > As a result, photographs of pedestrians caught in the act, along with their names and social identification numbers, are now instantly displayed on LED screens installed at Shenzhen road junctions.
        >
        > At some crosswalks, a brake-sounding alarm even goes off if someone walks when the pedestrian light is red, reportedly to alarm the jaywalkers and capture their photo in a moment of panic.[23]

        The report cited above includes a short piece of footage showing the system in operation.

    c. It has been reported that the US Navy is equipped with smart goggles that may be worn by troops. These can visually identify people from a database containing millions of biometric templates. This identification can be made from a distance as far as 19 km.[24]

32. The intrusions into citizens' privacy that are enabled by facial recognition technology are real, and they are profound. It has been said that the technology may herald 'the end of anonymity.'[25] For that reason, particular care needs to be taken to ensure that the use of biometric technologies, including facial recognition technologies, is strictly controlled.

5 Human Rights Framework

33. Allowing personal information to be collected, stored and used, including by disclosure to others, impinges on the right to privacy protected by article 17 of the ICCPR.

34. The Identity Bill is also likely to interfere with a number of other rights. While this submission focusses on the right to privacy, several other rights are mentioned below to provide a fuller idea about the potential scope of the limitations the Identity Bill may have on human rights.

5.1 Article 17 — the Right to Privacy

35. Article 17 of the ICCPR provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

36. The right to privacy is also protected in equivalent terms in a number of national and regional human rights instruments, and the jurisprudence of the superior courts that interpret those instruments can provide useful guidance about the content of article 17.

37. The concept of privacy has not been comprehensively defined in international law. Early writing described the right to privacy as the 'right to be left alone.' More recent discussions of privacy accept that the concept can assume slightly different connotations in different areas of life, and includes what has been termed 'informational privacy', which includes

> the right of the individual to limit access to personal information which represents any information that could be used in any way to identify an individual.[26]

38. In a similar vein, the ALRC has identified two types of privacy impingement: intrusion upon seclusion, and misuse of private information. The opportunities for each of these impingements to arise, and to rise to the level of an infringement, expand in the digital age.[27]

39. Both the Supreme Court of the United Kingdom and the European Court of Human Rights have confirmed that the collection, retention, and use of photographs and biometric identifiers such as fingerprints engage the right to privacy.[28] This is consistent with the fact that the *Privacy Act 1988* (Cth) recognises that biometric templates and biometric information used for the purposes of identification or verification are 'sensitive information.'[29]

40. The Statement of Compatibility with Human Rights acknowledges that the right to privacy is engaged by the Identity Bill.[30]

41. Some measures which limit the right to privacy may be justified. For that to be the case:

    a. **The measure must be prescribed by law.** That includes a requirement that the measure is legislatively defined with sufficient precision to enable people to understand its operation in advance, and to plan their conduct accordingly. The United Nations Human Rights Committee has further stated that where laws authorise the interference with privacy, 'a decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.'[31]

    b. **The measure must be directed towards a legitimate aim.** Such an aim must not be inconsistent with the essence of the right to privacy, or other rights protected by the ICCPR.

    c. **The measure must be necessary.** That means both that the legitimate aim could not be achieved without the measure, and could not be achieved in a way that is less intrusive on the right.

    d. **The measure must be proportionate.** That requires making an assessment of the importance of the objective and the extent of the limitation on the right.[32]

5.2 The right to privacy and biometric identification

42. Biometric systems limit the privacy of individuals in a number of ways. First, the collection, retention and disclosure or other use of a photograph, or a biometric template, will itself limit the informational privacy of an affected person. Secondly, biometric systems, particularly those designed to identify unknown persons, will return false positives and release private information about parties who are not the intended subject of the identification request. Thirdly, further sensitive information may be able to be extracted or inferred from biometric identifiers. For instance, information about age, race, sex and health may be deducible from facial images. Fourthly, biometric systems may facilitate privacy-limiting measures, including the collection and collation of large amounts of other information about the individual, as well as the surveillance and tracking of the individual. These last two features of biometric systems create a risk that profiling may take place on the basis of factors such as age, sex and race.[33] This last fact may engage the right to non-discrimination protected under article 26 of the ICCPR.

43. In recognition of the intrusions on privacy (as well as a number of other rights) that may be entailed or facilitated by the use of biometric systems, specialist international bodies and experts have identified measures that should, where possible, be implemented to minimise those intrusions. These include:

    a. Biometric systems should only be used where strictly necessary. In general, 'general security' will not warrant their use.[34] They should not be employed simply for the sake of convenience.[35] This is both because the systems are themselves intrusive of privacy, and because the risk of identity theft increases with greater use of the systems.[36]

b. Where possible, biometric systems should avoid storing source information, such as facial images, and instead deal only with biometric templates. With the right system designs, these may be 'renewable'. This architecture can therefore mitigate risks associated with identity theft.[37]

c. Where possible, centralised databases of biometric information should not be created. Such databases may be well protected, but 'any database is under the risk of being hacked or the data being compromised whatever technical, organisational or regulatory measures have been taken.'[38] Large centralised databases create a valuable prize and therefore a prominent target for those seeking to engage in identity theft. A former Privacy Commissioner has referred to this as the 'Fort Knox' effect.[39]

d. 'Function creep' must be avoided. Where biometric information is collected for one purpose, it should not retained or used for other purposes.[40] This principle – that personal information generally should be used only for the primary purpose of collection — is central to Australian privacy law.[41]

e. To minimise intrusions on privacy, as well as the risk, and the consequences, of fraud or data theft, as little biometric and other personal information should be collected as possible — the minimum required to achieve the purpose for which the data is collected.[42]

f. Where records of biometric data are kept for one legitimate purpose, it is not permissible to simultaneously collect or retain other biometric data because it might be useful for a different, illegitimate purpose.[43]

g. Using biometric systems for identification purposes is more intrusive of privacy than using it for verification purposes. Therefore, 'verification problems should not be solved with identification solutions.'[44]

h. Where the primary purpose for which biometric information has been collected has been fulfilled, the information should be deleted.[45]

i. Biometric systems should only be used to verify identity in the context of service delivery where alternatives are provided for those unable to be enrolled in those systems. Otherwise, the systems may have a discriminatory effect.[46]

j. To the extent possible, biometric data should only be collected, retained and used with the full and informed consent of the person affected. The person must be informed of all uses to which the information collected may be put. A genuine alternative must be available to the provision of the information. Where a person is given a choice between using a service and not providing biometric data, that is a strong indicator that information will not be collected with true consent.[47]

44. Regimes permitting the collection, retention and use of photographs and biometric information, and the compatibility of those regimes with the right to

privacy, have been considered on several occasions under the *European Convention on Human Rights*.[48]

45. In the case of *R (on the application of RMC) v Metropolitan Police Commissioner*,[49] the Supreme Court of the United Kingdom considered the retention of photographs, fingerprints and DNA samples by police. Police had obtained these from two persons (one of whom was a minor) in the course of their investigation of two offences. They did not proceed to prosecute either individual. However, the police did not destroy/delete the samples and the information they had collected. Instead, they followed their usual practice which was to retain that material on an indefinite basis. The information was then available for use in future criminal investigations. The Court held that the retention of this information engaged the right to privacy. Further, that retention was not necessary and proportionate in circumstances where the people affected had not been prosecuted, let alone convicted, of any offence. The European Court of Human Rights made a similar finding in *S v United Kingdom*.[50]

46. In a significantly earlier case, the European Commission of Human Rights (a former tribunal sitting below the European Court of Human Rights) had held that the police taking, and retaining, a photograph of an unidentified person at a public protest did not, in the circumstances of the case, impermissibly interfere with the right to privacy of that individual. In reaching that finding, the Commission emphasised that 'the authorities had taken no steps to identify the persons photographed by means of data processing'.[51]

5.3 Interference with other rights

47. While this submission focuses on the right to privacy, the Bill is also likely to interfere with a number of other human rights. Several of these are mentioned briefly below. One particular concern is that the Bill will place many Australians in the position of having to 'choose' whether to enrol their data with various government agencies.

(a) Example 1 — freedom of movement

48. If an Australian citizen wishes to travel abroad, they must obtain a passport. In doing so, they must provide personal information to the Department of Foreign Affairs and Trade, including biometric information in the form of a high-quality photograph. If the Identity Bill is passed, that information will be made available for use by the identity-matching services. The person's image and biographic information will therefore become searchable by (at least) law enforcement agencies and intelligence agencies.

49. Similarly, a person cannot in general travel abroad or return home except by 'vessel' through a 'port' (as defined in the Migration Act to include airports and aircraft respectively). In so doing, they may be required to provide personal identifiers or other information which may be collected by the Department of Home Affairs. Should the Identity Bill pass, that information will be made available for use by the identity-matching services.

50. In some cases, a person may have little true 'choice' about whether to travel (for instance, their family circumstances may make travel necessary). In other cases, people may be deterred from travelling because they do not wish their privacy to be infringed in the ways the Bill would allow. That may have a chilling effect on them exercising their freedom of movement (protected by article 12 of the ICCPR). To the extent that this choice arises as a result of an infringement on the right to privacy by Australian law, it would self-evidently infringe also article 12 of the ICCPR.

51. Further discussion of the kinds and sources of identification information that are within the purview of the Bill is contained later in this submission.

(b) Example 2 — the right to non-discrimination

52. The Explanatory Memorandum makes clear that it is envisaged that identity-matching services under the bill may be used by both government agencies and private organisations to streamline service delivery. That might be by making it easier for those requesting services to prove their identities. However, it could also be envisaged that biometric identifiers could be used in place of 'passwords' to access a variety of services (either on-line or off-line).

53. Most people can 'use' facial recognition technologies. However, this may pose problems for people who subsequently undergo surgery, are affected by disease, or even, in some cases, as they age.[52]

54. The Bill envisages Ministerial rules could make other biometrics available for use in the provision of identity-matching services. These other biometrics may also not be usable by different groups of people. For instance, manual workers and older people are more likely to experience difficulties in being recognised by fingerprint-matching technology. Some people have lost fingers or hands in accidents, or are born without them.

55. For this reason, the use of biometric technologies, including for the verification of identity, can engage the right to non-discrimination. It is essential that in all cases where biometric systems are employed to verify identity in the course of accessing a service, alternatives are provided to ensure that people are able to access that service on an equal basis.

(c) Example 3 — the right to a fair trial

56. It is unclear to what extent responses to requests for identity-matching services might be used, or admissible, in legal proceedings. The Intergovernmental Agreement on Identify-Matching Services,[53] which the Bill is intended to implement, states that 'the results of the Identity-Matching Services are not designed to be used as the sole basis for ascertaining an individual's identity for evidentiary purposes.' However, while this may not be the intent, the Bill does not restrict agencies from attempting to use the results of these services in that way.

57. Any such attempts might place a defendant in a difficult position. The secondary materials indicate that no identifying data will be retained in the

interoperability hub in relation to searches conducted through it. (This hub and other features of the Bill are described later in this submission.) That could conceivably make it difficult for defendants in criminal proceedings properly to interrogate, and therefore challenge, the results obtained. As noted above, biometric systems can give a false appearance of infallibility, and their use in judicial proceedings can therefore be misleading. Any prejudice to the rights of defendants to interrogate and challenge in a robust manner all biometric evidence that might be used in criminal proceedings against them would potentially interfere with the right to a fair trial, embodied in article 14 of the ICCPR.[54] Careful consideration should therefore be given to what, if any, use results derived from identity-matching services should be able to be put in judicial proceedings.

6 The Bills

58. Two bills are the subject of the current review: the Identity Bill and the Passports Bill.

59. This submission primarily addresses the Identity Bill. The principal immediate effect of the Passports Bill would be to enable information collected and held by the Department of Foreign Affairs and Trade to be made available for use under the regime that would be established by the Identity Bill, and to enable passports-related information to be shared automatically by computer.

6.1 The Identity Bill

60. The Identity Bill would:

a. permit the Secretary of the Department to 'develop, operate and maintain' the 'NDLFRS' (a note in the Bill explains that the term 'NDLFRS' is an acronym for 'National Driver Licence Facial Recognition Solution', but that compound term is not itself used in the operative text of the Bill)[55]

b. permit the Secretary of the relevant Department to 'develop, operate and maintain' the 'interoperability hub'[56]

c. define a number of 'identity-matching services' which are to be provided via the inter-operability hub[57]

d. allow the Minister to make rules defining new identity-matching services that could be provided through the interoperability hub[58]

e. allow the Minister to make rules defining new kinds of 'identification information' which could be either included in the NDLFRS and/or made available to (and through) the interoperability hub.[59]

6.2 The NDLFRS

61. The NDLFRS would consist of a database of 'identification information' that is also contained in state and territory-issued 'government identification documents', together with a system of biometric comparison of facial images.[60]

62. The NDLFRS would constitute a single, central repository for information related to identification documents that are issued by state and territory agencies.

63. The NDFLRS would then constitute one of the sources of identification information that would be able to be accessed by the identity-matching services provided via the interoperability hub.

64. The Explanatory Memorandum states that initially the NDLFRS will include the information held in state and territory driver's licence databases. However, it is envisaged that it may be expanded to include information associated with other state and territory licensing and identity regimes, including fishing, firearm and marine licences, proof of age and identity cards.[61]

6.3 The interoperability hub

65. The 'interoperability hub' is stated to be a 'facility … for relaying electronic communications between bodies and persons for the purposes of requesting and providing identity-matching services.'[62]

66. It is a striking feature of the Bill that it contains no further details about the nature of the hub. As long as what the Secretary devises can be characterised as a 'facility', and it has the function of relaying 'electronic communications' (a term defined very broadly in the Bill), and serves the purpose specified, the Secretary is empowered to implement and operate it. There are no further constraints on the design of the hub.

67. The Explanatory Memorandum states that the interoperability hub will feature a 'hub and spoke' model, and that no identification information will be 'permanently' stored in it.[63] Those constraints, however, are not contained in the Bill.

68. As will be discussed below, the extent of intrusion on privacy involved in any biometric system may be greatly affected by the design of that system. Virtually all aspects of the design of the hub are left to the Secretary to 'develop.' Even if the hub as first developed does not retain 'identification information', (whether that be as part of an indexing system, a result of caching, for later auditing or development purposes, or otherwise) there is nothing to prevent the Secretary from altering that design at a later time.

69. This lack of detail about the key features of the 'interoperability hub' is not consistent with the requirement that measures that limit human rights be prescribed by law. If the Bill is to proceed, the Commission considers that the core elements of the design of the interoperability hub should be specified in the text of the Bill, rather than be left entirely to the discretion of the Secretary.

6.4 Identification Information

70. Each of the identity-matching services defined in the Identity Bill involves the disclosure of 'identification information' by way of electronic communication via the interoperability hub. The concept of 'identification information' is therefore central to the Identity Bill.

71. 'Identification information' is defined broadly.[64] It is defined in two ways:

a. by reference to particular types of information. These include:

- a name by which an individual is or has been known
- a current or former address of an individual
- the place or date an individual was born
- the age of an individual (whether expressed by reference to a range or not)
- the current or former sex, gender identity or intersex status of an individual
- information about whether an individual is alive or dead
- an individual's current or former citizenship
- information about a visa an individual holds or held
- a facial image of an individual, a biometric template derived from such an image or a result of biometric comparison involving such an image.

b. by reference to particular repositories or sources of information. The relevant categories of information include:

- any information contained in a driver's licence, or any information 'associated with' such a licence
- any information contained in, or 'associated with' any other licence or document that contains a personal photograph and is issued to assist an individual to prove their identity
- any information contained in, or 'associated with', any document issued by the Minister administering the Migration Act to assist an individual to prove their identity
- any information contained in an Australian or foreign passport or travel document, or any information 'associated with' such a document by the Department administering the Australian Passports Act, or by any Department authorised to inspect or

seize the document (this would most obviously include the Department of Home Affairs).[65]

(A discussion of the types of personal information that fall within these categories is provided later in this submission.)

72. Most of the identity-matching services created by the Bill involve the use of a variety of identification information including a facial image, and the use of biometric analysis of that image for the purpose of verifying or establishing identity.

73. The Identity Bill would also permit the Minister to make rules defining new forms of identification information.[66] The Minister would also be required to consult the Human Rights Commissioner and the Information Commissioner before making any such rules.[67]

74. To make such rules, the Minister must be satisfied that the information:

a. could be used alone, or in conjunction with other information, to identify an individual

b. 'is reasonably necessary to provide one or more identity-matching services', and

c. 'would assist in one or more identity or community protection activities'.[68]

75. The Bill contains a list of 'Identity or community protection activities.' While the list is exhaustive, many of the items encompass a broad range of activities. They are:

a. 'preventing and detecting identity fraud'

b. 'law enforcement activities', which include 'preventing, detecting or prosecuting' offences against any federal, state or territory laws

c. 'national security activities', which include 'conducting an investigation, or gathering intelligence, relevant to Australia's national security'

d. 'protective security activities', which include 'promoting the security of an asset, facility or person associated with government'

e. 'community safety activities', which include 'promoting community safety' by identifying persons who have suffered, or are 'reasonably believed to be at risk or suffering, physical harm', as well as missing or dead persons

f. 'road safety activities', including 'promoting road safety' and 'promoting the integrity of the driver licensing systems'

g. verifying the identity of individuals.[69]

76. The Explanatory Memorandum makes clear that this rule-making power would authorise the Minister to specify new kinds of biometric information about individuals to be used in providing identity-matching services.[70]

77. Of particular concern in relation to this rule-making power is the breadth of the definition of 'identity and community protection activities.' Some reasons that is a matter of concern are:

    a. Allowing identification systems, and especially automated biometric identification systems, to be used to 'assist' in the 'prevention or detection' of crime appears to contemplate intrusive surveillance of persons (or, indeed, of the community at large) before any crime has been committed, and indeed potentially before there is any reason to believe that a particular crime will be committed.

    b. The nature of 'intelligence' is such that it may encompass the collection of very large amounts of data to identify and assess potential security risks. The range of information that could conceivably 'assist' in 'gathering intelligence' is very broad indeed.

    c. The activity of 'verifying the identity of individuals' cannot of itself justify the privacy-limiting measures that are inherent in this activity. It can only be justified by reference to some other aim — that is, if the verification is performed to serve some other legitimate purpose.

78. A further concern is whether some of the identity or community protection activities above are of sufficient importance to justify making further categories of information available to the identity-matching regime with the further limitations on privacy that that would entail.

79. The Minister would necessarily have very broad discretion in satisfying himself whether particular forms of information are reasonably necessary to provide an identity-matching service. However, the true impact of this rule-making power is revealed when it is read in conjunction with the Minister's power to make rules defining new identity-matching services. Together, these rule-making powers would give the Minister a broad discretion to increase dramatically the scope of the Identity Bill. This issue is discussed further below in conjunction with the Minister's power to define additional identity-matching services.

6.5 The Identity-matching Services

80. The Bill would allow the interoperability hub to be used to provide a number of 'identity-matching services'. These are:

    a. the FIS

    b. the FRAUS

    c. the FVS

    d. the IDSS

e. the OPOLS

f. such further services as may be specified in rules made by the Minister.[71]

81. Notes in the Bill state that these are acronyms with the following significance:

a. FIS: 'Face Identification Service'

b. FRAUS: 'Facial Recognition Analysis Utility Service'

c. FVS: 'Face Verification Service'

d. IDSS: 'Identity Data Sharing Service'

e. OPOLS: 'One Person One Licence Service'

However, these phrases or descriptions do not appear in the operative text of the Bill.

82. Each of these services is discussed in turn below.

(a) The FIS

83. The FIS is the most intrusive of the contemplated identity-matching services. A FIS is defined to be any service that 'involves comparing':

a. a facial image of a person (possibly, but not necessarily, together with other identification information) that is supplied with a request, and

b. identification information about that person contained in one or more of kinds of identification document specified in the request.[72]

84. Requests are made through the interoperability hub.[73]

85. Requests under the FIS must be made 'for the purpose of identifying an individual', or 'determining whether an individual has multiple identities.' They may only be made for 'community protection activities' (see above), and may only be made by agencies specified in the Bill. The agencies permitted to make requests include the Australian Border Force, the Australian Federal Police, the Australian Security Intelligence Organisation, state and territory police forces, and various other law enforcement, criminal intelligence and anti-corruption bodies.[74]

86. The Explanatory Memorandum provides significantly more information about the intended operation of the FIS. It explains that the FIS is intended to be used primarily to identify unknown people. It will do so by permitting 'one-to-many' searches for matches for facial images submitted by requesting agencies. That is, a requesting agency may submit a facial image (possibly together with other identification information) to the interoperability hub and request that it be compared with the facial images held in any or all of the databases accessible by the hub. The facial-matching process will

> return a small gallery of the of the highest matching facial images in the database. The receiving agency will then need to review the gallery and select a limited shortlist of possible matches. Only then will the receiving agency have access to the biographic details (such as the name) associated with the facial images on their shortlist, for further examination.[75]

87. That is, the response to a FIS request is a two-stage one. At the first stage, photographs of a number of people will be returned to the requesting agency. Necessarily, all but one of those people will not be the subject of the request. It could well happen that none of them are. The requesting agency then selects a subset of those matches. It appears (though it is not clear in the Explanatory Memorandum) that all the identifying information about each of those matches will be supplied to the requesting agency. Again, at most one of those persons will be the actual subject of the request. This system will represent a very significant intrusion into the privacy of the persons affected, and may, to borrow the language of the Explanatory Memorandum cited above, make them subject to 'further examination.' This fact, as the Nuffield Council on Bioethics has observed, gives lie to the platitude sometimes deployed that if a person has not done anything wrong, they have nothing to fear from regimes that limit their privacy.[76] That is even without observing that privacy should be regarded as an intrinsic, and not merely instrumental, good.[77]

88. None of the features of the FIS described in the two paragraphs above is contained in the Identity Bill. Under the Bill, it would be open to the Secretary to implement the interoperability hub in such a way that all of the information held about each individual in the first 'gallery' would immediately be supplied to the requesting agency. It would be possible to implement a version of the FIS where the requesting agency were able to request the number of matches to be returned, or the level of accuracy to be applied by the biometric facial matching software in determining which images or other identification information to return to a requesting agency. If this were permitted, the requesting agency could request that a low level of accuracy be applied, which would result in information about a larger number of people being returned to it.

89. There is nothing in the Identity Bill that controls what use may be made of the information returned at either of the two stages above. It would be possible for the receiving agency to capture and retain it for their own records — or even to compile their own databases of information they receive for future use in unrelated matters. It is relevant to note here that the Identity Bill places no limits on the number of FIS requests that may be made.

90. The Statement of Compatibility with Human Rights prepared in relation to the Identity Bill states:

> The agencies that will have access to the FIS are listed in the Bill and are limited to agencies that have national security and law enforcement functions, including Commonwealth and state and territory anti-corruption agencies. These agencies perform vital work to keep Australians safe from harm, and the effectiveness of these agencies is essential to protect the rights and freedoms of innocent members of the community. By specifying these agencies, the Bill will ensure that the right to privacy of individuals is only

> limited insofar as it is necessary to achieve the legitimate objectives of these agencies.
>
> To further limit the imposition on the right to privacy, the FIS will only be able to be used by these agencies for the purposes of preventing and detecting identity fraud, law enforcement, national security and protective security activities, and community safety activities.
>
> The availability of the face identification service for these purposes recognises the increased need to identify unknown individuals in these circumstances in a timely way, to limit the risk of harm to the community as a result of failure to identify an individual. For example, circumstances captured by these purposes may include identifying a child sex offender from child exploitation material, identifying suspects in hostage or siege situations, identifying gang members and associates, identifying suspected criminals from CCTV or other footage, or identifying a person who may pose a risk to public health or safety.
>
> The risk of harm arising from these types of situations justifies the increased imposition on the privacy of individuals that the FIS involves. By contrast, the results of failure to identify an individual in the course of road safety activities and verifying identity (primarily use for service delivery activities) are less severe and do not justify the increased privacy implications of the FIS. As such, the Bill does not allow the FIS to be used for those activities.[78]

91. This passage could be misleading. The limits on the use of the FIS relating to the need for a 'reasonable belief' of a risk to the public apply only to FIS requests relating to 'community safety activities'. There is no such qualification on the circumstances in which requests may be made for 'law enforcement activities' or 'national security activities.' It would appear to be entirely consistent with the Bill for the FIS to be implemented in such a way as to allow real-time (or virtually real-time) monitoring of CCTV footage to identify all people in public places if that were done for the purpose of preventing or detecting crime. Further, FIS requests may be made for the purpose of preventing, detecting, investigating or prosecuting *any* offence against laws of the Commonwealth, a State or a Territory. This would allow the FIS to be used to issue traffic infringement notices, or fines for littering or jaywalking. These are not fanciful applications: face recognition technology is capable of being applied in this way. Applications such as these are already in use in some foreign jurisdictions, including the UK and China.[79]

92. It may well be that there are circumstances in which the use of a service such as the FIS is warranted, despite the serious intrusions it would entail. Examples may include the investigation of serious crimes, or the need to prevent serious harm in the event of a reasonably anticipated event such as a terrorist attack. However, the use of such a measure must be strictly controlled to ensure that it is employed only when demonstrated to be justified. For this reason, if the Identity Bill proceeds, the Commission considers that it would be appropriate to introduce a warrant regime regulating access to the FIS.

93. As is observed at a number of points in the discussion above, many of the key aspects of the FIS are not contained in, or regulated by, the Bill. That is not consistent with the requirement that measures which limit human rights must be prescribed by law. The Commission considers that if the FIS is to be

retained in the Bill, the relevant provisions should be substantially redrafted so that its features and operation are fully described in and controlled by the Bill, rather than being left to the Secretary to 'develop.'

(b) The FRAUS

94. The 'FRAUS' is defined to be a service that allows a state or territory authority that has supplied identification information to the NDLFRS to make a request containing a facial image to the interoperability hub or directly to the NDLFRS. The facial image supplied with the request is to be compared with identification information in the NDLFRS that was supplied by the requesting agency. The request must be made for the purpose of 'assessing the accuracy or quality of identification information held by the requesting authority.'[80]

95. The FRAUS is a significantly more limited service than some of the others created by the Bill, and consequently does not appear to present such significant human rights concerns. However, the Bill does not make clear precisely how the FRAUS would operate. In particular, it is not clear what information would be supplied in a response to a FRAUS request, and whether it might include information about more than one person. Those matters are not addressed in the secondary materials. The Commission submits that those matters should be clarified in the text of the Bill so that a full assessment of any privacy impacts can be made.

(c) The FVS

96. The FVS is defined to be a service that 'involves' electronically comparing identification information provided by the person or body making the request with identification information that is contained in a government identification document. The FVS request must specify the kind of identification document that will be used in the comparison. A facial image must be included with the request, or in the response to the request. The comparison must be for the purpose of verifying the identity of an individual. Finally, the request and the response must be conveyed via the interoperability hub.[81]

97. FVS requests may be made by federal, state and territory authorities, local government authorities and non-government entities.[82]

98. The Explanatory Memorandum states that the FVS will provide 'different types of functionality':

> For example, in one case, the requesting agency may submit a person's facial image and other identification information (i.e. biographical information). The image is compared against a facial image on a government identification document associated with the same biographical information and a 'match' or 'no match' response is returned to confirm whether the facial images match. In some circumstances, the response may also contain identification information relating to the person, such as the person's image or other biographic information, where the requesting agency has a lawful basis to collect that information.

> In another case, the requesting agency may submit identification information about a person that does not include a facial image (biographical information only), and the service will return a copy of a facial image associated with a government identification document with the same biographical information.
>
> The second case may occur for example where a police officer wishes to conduct a driver licence check and is unsure as to the veracity of the licence document. The officer may submit the licence number and biographic details as a FVS service request and receive a copy of the facial image of the licence in that name, and compare it to the driver to verify their identity.[83]

99. It is noteworthy that none of this detail is included in the Bill. The Bill, on its face, does not explicitly prevent other variations of the FVS. For instance, a request might include limited biographic information, and return a photograph and a complete set of biographic information held about an individual.

100. The Explanatory Memorandum further states that private entities will only be able to access the FVS in a way that provides them with 'match or no match' responses, and will not involve the disclosure of any photographs of biographic information to the maker of the request.[84] This limitation, too, is not expressly provided for in the Bill.

101. As has been observed a number of times in this submission, measures that limit privacy must be provided for by law. Any such law must precisely define the measure, as well as any limitations or other protections against its overbroad application. It is of particular importance that the Bill specify whether, and if so, in what circumstances, the FVS will be permitted to return responses other than 'match or no match' responses.

102. Access to the FVS may only be given to local government and non-government entities if a number of further criteria are met. Those include that verifying identity is 'reasonably necessary' for one of the entity's functions or activities, and that the affected individual consents to the disclosure. These further requirements are, as far as they go, positive. It is not obvious, however, that they would, in practice, provide significant protections for individuals' privacy. That is so for several reasons.

103. First, it is unclear when it might be said that the verification of identity is 'reasonably necessary' for an activity undertaken by a private entity, and how and by whom that requirement would be enforced. Further, private entities can determine for themselves what activities they will engage in, and, in general, have a very wide discretion in deciding what they require in order to do so.

104. Secondly, private entities commonly request the voluntary production of personal information, or the authorisation to access personal information, as a precondition to providing a service. In many cases a person does not have any real choice about whether to access the service (for example, a bank card).[85] The requirement for consent in the Bill may therefore not provide any real protection for individuals' privacy.

105. While not specified in the Bill, it is envisioned that access to the FVS will be provided to private entities on a fee-for-service basis.[86] The Council of Europe

has noted that this may incentivise public agencies to disclose greater amounts of personal information than might be consistent with the right to privacy of affected individuals.[87]

106. Information available on the Attorney-General's Department website indicates that the FVS, one of the services 'created' under the Bill, is, in fact, already 'operational', and is 'providing access to passport, immigration and citizenship images'.[88] The website further states that the FIS 'will come online (for Commonwealth images in the first instance) in early 2018.'[89] It is unclear whether it will do so regardless of the passage of the Bill.

(d) The IDSS

107. A note in the Bill observes that 'IDSS' is an acronym for 'Identity Data Sharing Service', though that is not a phrase that appears in the operative text of the Bill.

108. While the IDSS is defined to be an 'identity-matching service', in fact it does not involve any matching of information.[90] Rather, the IDSS is a service that allows a federal, state or territory authority to disclose identification information about an individual to another federal, state or territory authority, via the interoperability hub. Any such disclosure must be made for the purpose of an identity or community protection activity. As noted above, that encompasses a wide range of activities. The Explanatory Memorandum suggests that the IDSS could be used to make bulk transfers of identification information between participating agencies. The Statement of Compatibility with Human Rights states that the IDSS will allow such transfers to be made in a secure efficient, accountable and transparent manner.[91]

109. The Statement of Compatibility with Human Rights suggests that the IDSS will have minimal human rights impacts because the sharing of data between government agencies is already permitted under other legislation, and the IDSS will allow this to happen in a more accountable and transparent way.

110. The mere fact that the IDSS will only authorise transfers of information which are legally authorised under other statutes does not mean that the IDSS will have no impact on the right to privacy. In facilitating large transfers of identification information, the IDSS may magnify the extent of any interference with that right.

111. In any event, the Identity Bill does, in section 19, contain a provision which would have the effect of making lawful certain disclosures of information that would not, in the absence of section 19, be lawful. Further, the Passports Bill would have the effect of increasing the extent to which identification information relating to passports could be disclosed.

112. One, perhaps extreme, hypothetical example may help illustrate the way in which the IDSS may intrude on the right to privacy. If, at some stage in the future, a law enforcement body or an intelligence agency decided that holding all of the information available through the interoperability hub in its own, stand-alone, database could be useful to 'prevent offences', or to 'gather intelligence' relevant to national security (for instance, for use in a mass-scale

automated biometric surveillance system, such as 'smart CCTV'), it would be open to that agency to request other government agencies to transfer their entire databases of identification information via the IDSS. The Commission does not suggest that a mass transfer of this kind is contemplated. However, the example illustrates the point that facilitating data transfers can negatively affect privacy.

113. The Commission acknowledges that the sharing of personal information between agencies may be warranted in some circumstances — for instance, where there are good reasons to believe that that will assist in the investigation of a crime, especially a serious crime. That is despite the fact that such disclosures of personal information will limit the right to privacy of affected individuals. However, as explained above, any laws authorising such disclosures should be precise in their terms and ensure that disclosures will only be possible where necessary and proportionate. The IDSS regime as drafted does not specify the circumstances in which disclosures may be made, nor the extent or types of information that may be disclosed. The Commission therefore submits that the IDSS regime not be passed in its current form. If the IDSS regime is to be implemented, the Bill should be amended to ensure that it permits disclosures of information only when necessary, and only to the extent necessary, to achieve a legitimate objective.

(e) The OPOLS

114. A note in the Bill observes that 'OPOLS' is an acronym for 'One Person One Licence Service', though that is not a phrase that appears in the operative text of the Bill.

115. A request for an OPOLS may only be made by a State or Territory authority that has provided information to the NDLFRS. The request must include a facial image of an individual, and may include further identification information. The service will compare the supplied information with identification information held in one of the state or territory databases held in the NDLFRS. The request may only be made by an agency that issues government identification documents, and the comparison made by the service may only be made against a database that holds government identification documents of the same kind. The comparison must be made for the purpose of determining whether a person holds multiple identification documents of a particular type in one or more States or Territories. The request may be made directly to the NDLFRS, or via the interoperability hub.[92]

116. The Explanatory Memorandum states that the OPOLS will be a 'constrained one-to-many' search facility,

> meaning it returns a gallery of a very small number of the highest matching facial images from identification documents of the same type across one or more jurisdictions. This means that the use of the OPOLS may have potential privacy implications for the individual that is the subject of the query, as well as a small number of other individuals whose images or identification information may be returned as possible matches to the query.[93]

117. Once again, it may be noted that important features of the OPOLS service are not mandated by the Bill. In particular, the nature of the service as a 'constrained one-to-many' service, and the nature of the response to a request, should be specified in the Bill.

118. The OPOLS service, like the FRAUS, uses information that has been collected for the purpose of issuing drivers' licences, and uses that information for the purpose of protecting the integrity of the licensing regime. That means that these services are using personal information for purposes connected to the purposes for which the information was collected. The OPOLS (and the FRAUS) therefore do not involve 'function creep' in the same way that the other identity-matching services do. The problem of function creep, common to a number of the identify-matching services, is discussed further below.

(f) 'such further services as may be specified in rules made by the Minister'

119. As well as the five identity-matching services discussed above, section 7 of the Identity Bill would authorise the Minister to make rules defining further such services. A service defined under these rules would be required to 'involve the collection, use and disclosure of identification information', and 'involve the interoperability hub or the NDLFRS.'

120. It may be observed that any new services created by the Minister would not be required to involve the interoperability hub. That is a point of distinction from most of the identity-matching services defined in the Bill. It means that the claimed justification that the Bill would allow for 'efficient', 'transparent' and 'accountable' use of identification information (because of design features of the hub) would not necessarily apply in relation to new services defined under section 7.

121. The Minister's power to create new services would include the power to determine both who could make requests under the service, and what categories of information they could request.

122. A new service could be created permitting requests for information to be made by government authorities. There are no further restraints on the Minister's rule-making power with respect to requests by government entities.

123. A new service could also be created permitting requests to be made by local governments or non-government entities. In such a case, the Minister would have to be satisfied of certain further matters, including that the purpose of a request is to verify an individual's identity; that verification of the individual's identity is 'reasonably necessary' for a function or activity of the requesting entity; that the affected individual has given consent for the request to be made, that the entity carries out activities in Australia, and is bound by the Privacy Act or some similar regime.[94]

124. The Commission makes the following remarks about the rule-making power insofar as it relates to local governments or non-government entities:

    a. Unlike a government statutory body, whose actions are constrained by legislation, it is unclear what would be considered to be 'reasonably

necessary' for the activities of a private entity, and in particular, a for-profit entity. This would potentially not place much real limit on requesting entities.

b. The remarks about 'consent' made above in relation to the FVS apply equally to the Minister's power to define new identity-matching services. There is a real risk that private entities will make access to services contingent on a person consenting to their identity being verified. In the case of many services, they will have little true choice about whether to provide their 'consent'.

c. It is likely that services would be made available to private bodies on a fee-for-service basis. The Commission refers to the remarks above in relation to the FVS about the incentives this may provide to agencies to increase disclosures of personal information.

d. There is nothing in the Bill that limits the Minister's power so that only services returning 'match/no-match' type results may be created in relation to non-government entities. That means that rules might be made permitting disclosure to private bodies of any of the identification information available through the NDLFRS or the interoperability hub.

125. The Minister's power to define new identity-matching services must be read together with the power to define new kinds of 'identification information.' As noted above, that power, too, is very broad. It would include the power to stipulate that new kinds of biometric information are identification information. Together, these powers could give the Minister the power to create new identity-matching services which are far more intrusive on privacy than those explicitly created by the Bill.

126. The Commission submits that it is inappropriate to give such broad rule-making powers to the Minister. It increases the probability that identity-matching services will not intrude on privacy only to the minimum degree necessary to achieve a legitimate end. It also reduces the degree of public and parliamentary scrutiny the measures might receive, which might provide some protection against the creation of new identity services that limit privacy to a disproportionate degree. Finally, such a broad rule-making discretion is arguably inconsistent with the principle that measures limiting human rights must be prescribed in detail by law. If it proves necessary at some later stage to create a new identity-matching service, or to define new kinds of identification information, that should be done as and when necessary by way of amendment to the relevant legislation.

127. The Commission therefore considers that the provisions empowering the Minister to make rules defining new categories of identification information, and creating new kinds of identity-matching services, should not be passed.

6.6 'Function Creep'

128. The identification information that may be accessed via identity-matching services has been collected under a number of statutes, including statutes regulating who is permitted to drive motor vehicles, which citizens are

permitted to travel outside Australia, and which non-citizens are permitted to enter Australia and the terms on which they are entitled to do so.

129. Some of the identity-matching services (the FRAUS and the OPOLS) would be provided for the purpose of ensuring the integrity of the information held by relevant licence-issuing agencies. That is a purpose that is consistent with the purposes for which the information was collected.

130. However, other identity-matching services, including the FIS, the FVS and the IDSS, would permit the use of sensitive personal information for wholly different purposes. As is discussed earlier in this submission, that amounts to 'function creep' and is particularly intrusive of affected individuals' privacy. Those individuals supplied personal information to licencing bodies with no knowledge, and no way of knowing, that it would be used as contemplated by the Bill.

131. It may, in some circumstances, be permissible to limit privacy in this way. In particular, where verifying a person's identity, or identifying an unknown person, would assist in investigating a serious crime, or preventing a specific anticipated serious crime, use of a service such as the identity-matching service might be warranted. However, the Bill does not limit the use of the services in this way. This is a further reason that the provisions creating the FIS, the FVS and the IDSS are overbroad. The Commission therefore submits that, if the Bill is to proceed, the provisions creating these services should be entirely redrafted to ensure they are used only when strictly necessary to respond to a pressing need.

7 What information would be available for use in identity-matching services?

132. In assessing the proportionality of a measure in order to determine whether the limitations it imposes on human rights are permissible, it is relevant to consider both the nature and the extent of those limitations. It is therefore relevant to observe that it appears that the majority of people in Australia — both citizens and non-citizens — will be affected by the Bill, in that the Bill would allow their identification information to be used and disclosed.

133. The following discussion attempts a preliminary survey of the information that would be accessible to the interoperability hub. Its purpose is to illustrate the extent to which the Identity Bill would intrude on the privacy of people in Australia.

7.1 Included databases

134. The interoperability hub allows for information to be shared in the provision of identity matching services.

135. The Explanatory Memorandum states that, initially, the data sets that will be available for matching purposes will be:

a. information held in the NDLFRS. As discussed above, the NDFLRS will consist of the information held in various state and territory databases. Initially, it is envisioned that information relating to drivers' licences will be included.[95] However, the Identity Bill would in fact allow state and territory agencies to provide for inclusion in the NDLFRS any identification information that is contained in 'government identification documents'. That would include information held by state and territory governments in relation to other licencing regimes. The definition of 'government identification document' would cover other forms of 'document' — the definition is potentially very wide.

b. citizenship and visa information held by the Department of Home Affairs.[96]

c. passport and other travel document information held by the Department of Foreign Affairs and Trade.[97]

7.2 Content of participating databases

136. The Commission has not had an opportunity to undertake a comprehensive review of all the information that may be contained in the databases that will initially be made available for identity-matching services. However, the following outline of some of the principal relevant legislation provides some idea about the extent of the information that would fall within the ambit of the scheme that would be established by the Bill.

(a) NSW 'driver licences'

137. Each State and Territory has its own driver licensing regime. The following discussion of the NSW regime is provided as an example of these regimes.

138. 'Driver licences' in NSW are issued under the *Road Transport Act 2013* (NSW), and the Regulations made under that Act. The *Road Transport (Driver Licensing) Regulation 2017* (NSW) states that the following information must be shown in each driver licence:

> (a) a licence number for the person to whom it is issued, and
>
> (b) the full name of the person, and
>
> (c) a photograph of the person, and
>
> (d) the person's date of birth, and
>
> (e) the person's residential address, and
>
> (f) the person's signature (or a reproduction of that signature), and
>
> (g) the class or classes of licence held by the person, and
>
> (h) the expiry date of the licence, and
>
> (i) the code of any condition to which the licence is subject.[98]

139. The legislation and regulations explicitly provide that the majority of the information above is to be kept in a register, and that photographs may be kept and used for a number of purposes.[99] The regulations further provide that the NSW driver licence register may also record 'other information':

> (a) for the purposes of the Act and this Regulation, or
>
> (b) for the purposes of another Act, or
>
> (c) for other purposes, as the Authority [Roads and Maritime Services NSW] considers appropriate.[100]

140. The relevant Authority is therefore given a wide discretion as to what information it chooses to record in its driver licence register.

(b) Australian Passports

141. Under the *Australian Passports Act 2005* (Cth), the relevant Minister may request an applicant for a passport to provide personal information relating to their application.[101] The Minister may make determinations allowing personal information about applicants to be requested from other persons and bodies. Those currently include the Australian Electoral Commission and any person who the Minister considers can provide information necessary to satisfy the Minister of the applicant's identity.[102] The Minister can make determinations about what kinds of information may be requested in relation to the issue of a passport. However, the Minister may request personal information even if no such determination has been made. Currently, the Minister is explicitly empowered to request any kind of personal information that is requested in a passport application form.[103] The current Ministerial Determination envisages that the information that may be held about passport applicants and holders will include:

> (i) the person's full name; and
>
> (ii) the person's date and place of birth; and
>
> (iii) the person's sex; and
>
> (iv) the number of any Australian travel document held by the person; and
>
> (v) the date and place of issue of any Australian travel document held by the person; and
>
> (vi) the person's address; and
>
> (vii) the person's occupation; and
>
> (viii) the person's signature; and
>
> (ix) a photograph of the person;

but may include any other 'details on a document or other thing that evidences or indicates, or can be used to evidence or indicate, the applicant's identity, citizenship or any aspect of the applicant's identity or citizenship'.[104]

157. As at 30 June 2016, 45 government agencies were using the DVS (though only one of the eight state and territory road agencies was using it). 350 private sector organisations were using it.[123] The Statement of Compatibility with Human Rights prepared in relation to the Identity Bill suggests that the FVS is intended to perform a similar (though augmented) function to the DVS.[124] It appears reasonable to assume that the FVS could be used at least as widely as the DVS.

7.5 How often would the identity-matching services be used?

158. Publicly-available documents suggest that were the Bill to pass, the identity-matching services it would enable would be used heavily.

(a) Precedent: the DVS

159. As noted above, the DVS has been available to government agencies since 2008, and, on a fee-for-service basis, to some private sector organisations since 2014. The Fee Schedule for 'Business Users' in relation to the DVS indicates that discounts are available for bulk users, with the cheapest rates available to entities making more than one million requests per annum.[125] This indicates that the DVS is widely used — or, at the least, that the government hopes or expects that it may be. As noted above, this would appear to be a good guide to the likely use of the FVS if the Bill were to pass.[126]

(b) Template MOUs for the use of identity-matching services by federal agencies

160. The template Memoranda of Understanding (MOUs) made available by the Attorney-General's Department in relation to National Facial Biometric Matching Capability indicate that agencies which make their data holdings available for use in those services will (subject to further agreement) agree to have a capacity to respond to 70,000 queries per day.[127]

(c) The Passports Bill

161. The Passports Bill contains a provision that would allow the relevant Minister to make arrangements allowing for computerised decision-making under the *Australian Passports Act 2005* (Cth).[128] The Explanatory Memorandum provides the following discussion of this provision:

> The services operate on an automated query and response basis. When data-holding agencies receive requests for information that satisfy parameters specified in bilateral data-sharing arrangements … **the requests will be processed and responses provided in a timeframe that precludes the exercise of human discretion in deciding whether to disclose the information in each case. The scale of expected future FVS use by large-client service agencies is a further factor that will make human intervention infeasible.** It will also allow law enforcement and national security agencies to act without delay to identify people in circumstances where their liberty and physical security, or the liberty and physical security of others, are under threat, and take time-critical action to prevent injury or loss of life.[129] (emphasis added)

(c) The Migration Act 1958 (Cth)

142. The Migration Act authorises the collection of evidence of identity in a range of circumstances. That information includes the following 'personal identifiers':

> (a) fingerprints or handprints of a person (including those taken using paper and ink or digital livescanning technologies);
>
> (b) a measurement of a person's height and weight;
>
> (c) a photograph or other image of a person's face and shoulders;
>
> (d) an audio or a video recording of a person
>
> (e) an iris scan;
>
> (f) a person's signature.[105]

143. The regulations can also provide for the collection of other personal identifiers, if their collection does not require an 'intimate forensic procedure,' and the identifier is 'an image of, or a measurement or recording of, an external part of the body.' [106]

144. Personal identifiers may be collected from citizens or non-citizens when they enter or depart from Australia.[107] Personal identifiers may also be collected from non-citizens in a variety of other circumstances. Of particular note is that persons in immigration detention are obliged to provide personal identifiers. Use of reasonable force may be applied if the person detained has refused to allow an identification test to be carried out.[108]

145. Virtually all of the information collected under these provisions will be information that is 'associated with' an 'Australian travel document or foreign travel document by an authority of the Commonwealth … by which the travel document may be inspected or seized under a law of the Commonwealth.'[109] Information collected and held under the Migration Act may also be 'information about a visa the individual holds or held'[110] and/or information about a person's 'current or former citizenship.'[111] It will include facial images.[112] All such information will be 'identification information' for the purposes of the Identity Bill and available for use in identity-matching services.

7.3 Number of people affected

146. A brief overview of the number of people whose identification information is held in the databases that will be available for use in providing identity-matching services is given below.

(a) Drivers' licences

147. These licences are held by a large number of people. The Commission has not, in the time available to prepare this submission, identified an authoritative Australia-wide source of statistical information about the numbers of people who hold these licences. The following discussion deals with information

relating to NSW, which would appear likely to be representative of the situation throughout the country.

148. As at 31 December 2017, there were 6,091,186 motor vehicle licences on issue in NSW. If rider licences are excluded (to allow for the fact a person may hold both a driver and rider licence), 5,487,447 licences were held in NSW at that date.[113] At the end of September 2017, the population of NSW was estimated to be 7,895,800.[114] The minimum age at which a driver's licence may be obtained in NSW is 16. In June 2014, there were approximately 1.4 million children in NSW under the age of 15.[115] Together, these figures suggest that over 84% of eligible people currently hold a driver's licence in NSW (and that it is quite possible that the figure is significantly higher). It is not unreasonable to assume that the numbers are roughly equivalent in other states and territories.

(b) Passports

149. It has been estimated that about half of Australians hold biometric passports.[116] Passports may be issued to children. It may therefore be said with some confidence that there are a significant number of passport holders who are not also holders of drivers' licences.

(c) Visas, non-citizens and immigration information

150. As at November 2016, there were an estimated 1,310,100 non-citizens in Australia over the age of 15 who held permanent or temporary visas, or whose status was 'not determined'.[117] All of these people hold visas, which have personal information associated with them that is held by the Department of Home Affairs under the Migration Act. It must be assumed that at least some of these people did not hold an Australian driver's licence.

151. Data on the Australian Bureau of Statistics website records that, in the year ended December 2016, there were '37.7 million crossings of Australia's international borders'.[118] These included 10 million Australian residents returning after short-term absences from Australia, 8.3 million visitors arriving for a short-term stay, 715,700 permanent and long term arrivals, 9.9 million Australian residents departing for a short duration, 8.3 million visitors leaving Australia after a short-term stay, and 448,700 permanent and long-term departures from Australia.

152. These figures are for a single year. They indicate that a large number of people, including Australian citizens, have passed through Australian immigration control, and therefore will have their personal information stored in Immigration databases. It would appear that this information would be information that is 'associated with an Australian travel document', associated with a foreign travel document, 'associated with' a document issued by the Department of Home Affairs, or 'about a visa.'

(d) Summary

153. While not a comprehensive survey, the figures above suggest that a very large proportion of people within Australia hold an 'identity document' that would fall within the categories of documents captured by the Bill. Their identifying information, including photographs, would therefore become available for search by relevant government agencies were the Bill to pass.

7.4 The DVS

154. The figures above are compounded by the fact that identifying information is already made available for identity-matching services under another service known as the DVS, or 'document verification service.' That allows for checks to be made to verify the authenticity of identity documents, but does not include a facility to compare facial images. The Explanatory Memorandum to the Identity Bill states that this service has been available to government agencies since 2009, and to private entities since 2015.[119] (A privacy impact assessment prepared in relation to the expansion of the DVS records that the DVS became available to some agencies in 2008, and to some private entities in 2013).[120] The documents that can be verified under the DVS include:

a. birth certificates
b. certificates of registration by descent
c. change of name certificates
d. citizenship certificates
e. driver licenses
f. marriage certificates
g. Medicare cards
h. passports
i. Immi Cards
j. visas.[121]

155. It appears that it has not been considered necessary to provide a legislative basis to operate the DVS (beyond the statutory powers participating agencies hold under their own legislation to collect, keep and disclose relevant information). The Identity Bill does not include the DVS. However, it is intended that the DVS will continue to operate alongside the identity-matching services that would be established by the Identity Bill.[122] This will increase the range of identity materials that are searchable by participating entities.

156. The DVS further expands the range of personal information that will be available to both government agencies and private bodies for verifying identity or identifying individuals.

162. Again, this demonstrates that the government expects that the identity-matching services will be widely used.

(d) Conclusion

163. While limited, the information above suggests that it is envisaged that the identity-matching services will be used extensively. This in turn suggests that, if passed, the privacy of a large number of people may be affected.

8 Conclusion and recommendations

164. On the basis of the analysis above, the Commission makes the following recommendations.

Recommendation 1

The Bill should not proceed in its current form.

Recommendation 2

If the Bill proceeds, it should be amended so that the core elements of the design and operation of the interoperability hub should be specified in the text of the Bill, rather than being left to the discretion of the Secretary.

Recommendation 3

If the Bill proceeds, the provisions defining each of the identity-matching services should be substantially redrafted, so that their functionality is fully defined in the Bill.

Recommendation 4

If the Bill proceeds, it should be amended so that access to the FIS is only available on the issue of a warrant.

Recommendation 5

If the FIS proceeds, it should be available only on the issue of a warrant.

Recommendation 6

If the Bill proceeds, it should be amended to ensure that any identification information disclosed in the response to a request for an identity-matching service is not retained beyond the time necessary to verify or establish identity.

Recommendation 7

If the Bill proceeds, it should be amended to ensure that identification information produced in response to a request for an identity-matching service is not used for any purpose other than establishing or verifying identity.

Recommendation 8

The Minister's rule-making powers in sections 5(1)(n) and 7(1)(f) of the Bill should not be passed.

Recommendation 9

If the Bill proceeds, the definition of 'identity or community protection activity' in section 6 should be amended so that:

- limb (a) of the definition of 'law enforcement activities' in subsection (3) includes only the prevention of *serious* offences
- subsections (7) and (8), dealing with 'road safety activities' and 'verifying identity' are deleted.

---

[1] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). At http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (viewed 22 March 2018).
[2] Roger Clarke, 'Just Another Piece of Plastic Your Wallet: The 'Australia Card' Scheme', *Computers and Society*, 18(1) (January 1988), 7, 16.
[3] Roger Clarke, 'Just Another Piece of Plastic Your Wallet: The 'Australia Card' Scheme', *Computers and Society*, 18(1) (January 1988), 7,18. See also the reference to the Australia Card Scheme in the context of a discussion of biometric identification in Malcolm Crompton, 'Biometrics and Privacy', [2002] *PrivLawPRpr* 36; (2002) 9(4) *Privacy Law and Policy Reporter* 68. Available at https://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/PrivLawPRpr/2002/36.html (viewed 28 March 2018).
[4] Explanatory Memorandum to the Identity Bill, 3 [7]-[8].
[5] Commonwealth, *Parliamentary* Debates, House of Representatives, 7 February 2018, 8 (the Hon Peter Dutton MP).
[6] See the Statement of Compatibility with Human Rights contained in Attachment A to the Explanatory Memorandum to the Identity Bill, 46-47.
[7] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 20-21. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).
[8] Australian Law Reform Commission, *For Your Information: Privacy Law and Practice*, Report 108 (May 2008), 406 [9.64]. Available at https://www.alrc.gov.au/publications/report-108 (viewed 28 March 2018).
[9] Australian Law Reform Commission, *For Your Information: Privacy Law and Practice*, Report 108 (May 2008), 406 [9.64]. Available at https://www.alrc.gov.au/publications/report-108 (viewed 28 March 2018).
[10] Mr Holger Haibach, Rapporteur to the Council of Europe Parliamentary Assembly, Explanatory Memorandum to *The need for a global consideration of the human rights implications of biometrics*, COE Doc 12522 (16 February 2011), 6 [2]. Available at http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=13103 (viewed 28 March 2018).
[11] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 4. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).
[12] National Consultative Ethics Committee for Health and Life Sciences, *Opinion No. 98 — Biometrics, identifying data and human rights* (26 April 2007), 4 (footnote 1). Available at www.ccne-ethique.fr/en/publicatoins/biometrics-identity-data-and-human-rights (viewed 13 March 2018).
[13] Malcolm Crompton, 'Biometrics and Privacy', [2002] *PrivLawPRpr* 32; (2002) 9(3) *Privacy Law and Policy Reporter* 53. Available at http://www.austlii.edu.au/journals/PrivLaw PRpr/2002/32/html (viewed 13 March 2018).

[14] Paul de Hert, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions', in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013) 369, 406.
[15] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors* (March 2013), 2. Available at https://www.priv.gc.ca/media/1765/fr_201303_e.pdf (viewed 28 March 2018); Canadian Human Rights Commission, *Identity Certification and the Protection of Human Rights* (August 2010), 10. Available at https://www.chrc-ccdp.gc.ca/eng/content/identity-certification-and-protection-human-rights (viewed 28 March 2018).
[16] Council of Europe, *Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric* data (2005), [31]. Available at https://rm.coe.int/16806840ba (viewed 14 March 2018).
[17] See eg the summary in Patrizio Campisi, 'Security and Privacy in Biometrics: Towards a Holistic Approach', in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013) 1, 7-10.
[18] Claus Vielhauer, Jana Dittmann, and Stefan Katzenbeisser, 'Design Aspects of Secure Biometric Systems and Biometrics in the Encrypted Domain', in Patrizio Campisi (ed*), Security and Privacy in Biometrics* (Springer, 2013)25, 26; Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 20. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018)..
[19] BBC News, *Malaysia car thieves steal finger* (31 March 2005). Available at http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm (viewed 28 March 2018). This type of attack on biometric systems has also been referred to by a former Privacy Commissioner: see Malcolm Crompton, 'Biometrics and Privacy', [2002] *PrivLawPRpr* 32; (2002) 9(3) *Privacy Law and Policy Reporter* 53. Available at http://www.austlii.edu.au/journals/PrivLaw PRpr/2002/32/html (viewed 13 March 2018).
[20] M Crompton, 'Biometrics and Privacy' [2002] *PrivLawPRpr* 32; (2002) 9(3) *Privacy Law and Policy Reporter* 52, available at http://www.austlii.edu.au/au/journals/PrivLawPRpr/2002/32.html (viewed 13 March 2018).
[21] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, 'Fingerprint Template Protection: From Theory to Practice', in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013) 187, 187.
[22] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* (Advance), 4. Available at http://www7.austlii.edu.au/cgi-bin/download.cgi/au/journals/UNSWLJ/2017/6 (viewed 23 March 2018).
[23] ABC News, *Chinese authorities use facial recognition, public shaming to crack down on jaywalking, criminals* (20 March 2018). Available at http://www.abc.net.au/news/2018-03-20/china-deploys-ai-cameras-to-tackle-jaywalkers-in-shenzhen/9567430 (viewed 23 March 2018).
[24] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors* (March 2013), 4. Available at https://www.priv.gc.ca/media/1765/fr_201303_e.pdf (viewed 28 March 2018).
[25] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 9. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).
[26] Patrizio Campisi, 'Security and Privacy in Biometrics: Towards a Holistic Approach', in Patrizio Campisi (ed), *Security and Privacy in Biometrics* (Springer, 2013) 1, 3.
[27] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report 123 (2014), Ch 5.
[28] *R (on the application of RMC) v Metropolitan Police Commissioner* [2010] 4 All ER 510; *S v United Kingdom* (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008).
[29] *Privacy Act 1988* (Cth) s 6.
[30] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill, 43.
[31] United Nations Human Rights Committee*, General Comment No. 16: Article 17 (Right to Privacy)—The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32nd Sess, HRI/GEN/1/Rev.9 (Vol. I), (1988) [8].
[32] United Nations Human Rights Committee*, General Comment No. 16: Article 17 (Right to Privacy)—The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32nd Sess, HRI/GEN/1/Rev.9 (Vol. I), (1988); ; United Nations Economic and Social

Council, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political* Rights UN Doc E/CN.4/1985/4, Annex (1985). An equivalent test is applied by courts interpreting the European Convention on Human Rights.

[33] Prof. dr. Paul de Hert & Koen Christianen, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* April 2013), 24. Available at https://www.coe.int/en/web/data-protection/reports-studies-and-opinions (viewed 28 March 2018).

[34] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 13. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[35] Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), Recommendation 3. Available at https://rm.coe.int/16806840ba (viewed 20 March 2018).

[36] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 17. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[37] Prof. dr. Paul de Hert & Koen Christianen, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* April 2013), Recommendation 5, p 6. Available at https://www.coe.int/en/web/data-protection/reports-studies-and-opinions (viewed 28 March 2018).

[38] Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), [50]. Available at https://rm.coe.int/16806840ba (viewed 20 March 2018).

[39] Malcolm Crompton, 'Biometrics and Privacy', [2002] *PrivLawPRpr* 36; (2002) 9(4) *Privacy Law and Policy Reporter* 68. Available at https://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/PrivLawPRpr/2002/36.html (viewed 28 March 2018).

[40] Prof. dr. Paul de Hert & Koen Christianen, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* April 2013), 6. Available at https://www.coe.int/en/web/data-protection/reports-studies-and-opinions (viewed 28 March 2018); Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 17. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[41] See, eg, *Privacy Act 1988* (Cth), Schedule 1, Australian Privacy Principle 6.

[42] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 33. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[43] Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), [34]. Available at https://rm.coe.int/16806840ba (viewed 20 March 2018).

[44] Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), [22]. Available at https://rm.coe.int/16806840ba (viewed 20 March 2018).

[45] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 10. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[46] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 15. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[47] Council of Europe Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies,* Doc 00720/12/EN WP193 (27 April 2012), 10-12. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (viewed 28 March 2018).

[48] *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature by the member States of the Council of Europe 4 November 1950, entered into force 3 September 1953.

[49] *R (on the application of RMC) v Metropolitan Police Commissioner* [2010] 4 All ER 510.

[50] *S v United Kingdom* (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008).
[51] *Friedl v Austria* judgment of 31 January 1995, Series A no. 305-B, opinion of the Commission; cited in *S v United Kingdom* (European Court of Human Rights, Grand Chamber, Application Nos 30562/04 and 30566/04, 4 December 2008), 24 [82]..
[52] Canadian Human Rights Commission, *Identity Certification and the Protection of Human Rights* (August 2010), 33. Available at https://www.chrc-ccdp.gc.ca/eng/content/identity-certification-and-protection-human-rights (viewed 28 March 2018).
[53] Intergovernmental Agreement on Identify-Matching Services (5 October 2017), available at https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf (viewed 26 March 2018).
[54] See eg Mr Holger Haibach, Rapporteur to the Council of Europe Parliamentary Assembly, Explanatory Memorandum to *The need for a global consideration of the human rights implications of biometrics*, COE Doc 12522 (16 February 2011), 9. Available at http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=13103 (viewed 28 March 2018); Prof dr. Paul de Hert & Koen Christianen, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (April 2013), [31] Available at https://www.coe.int/en/web/data-protection/reports-studies-and-opinions (viewed 28 March 2018).
[55] Identity Bill, s 15.
[56] Identity Bill, s 14.
[57] Identity Bill, ss 7-12.
[58] Identity Bill, s 7(1)(f).
[59] Identity Bill, s 5(1)(n).
[60] Identity Bill, s 15.
[61] Explanatory Memorandum to the Identity Bill, p 8 [21].
[62] Identity Bill, s 14.
[63] Explanatory Memorandum to the Identity Bill, p 28 [172].
[64] Identity Bill, s 5.
[65] Identity Bill, s 5.
[66] Identity Bill, s 5(1)(n).
[67] Identity Bill, s 5(4)(b)
[68] Identity Bill, s 5(4)(a)
[69] Identity Bill, s 6.
[70] Explanatory Memorandum to the Identity Bill, 19 [111].
[71] Identity Bill, s 7.
[72] Identity Bill, s 8(1)(a).
[73] Identity Bill, s 8(1)(c).
[74] Identity Bill, s 8.
[75] Explanatory Memorandum to the Identity Bill, p 22 [121].
[76] Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues* (September 2007), 33-34. Available at http://nuffieldbioethics.org/project/bioinformation (viewed 28 March 2018).
[77] Nuffield Council on Bioethics, *The Forensic Use of Bioinformation: Ethical Issues* (September 2007), 33-34. Available at http://nuffieldbioethics.org/project/bioinformation (viewed 28 March 2018).
[78] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill, p 51.
[79] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* (Advance), 4. Available at http://www7.austlii.edu.au/cgi-bin/download.cgi/au/journals/UNSWLJ/2017/6 (viewed 23 March 2018); ABC News, *Chinese authorities use facial recognition, public shaming to crack down on jaywalking, criminals* (20 March 2018). Available at http://www.abc.net.au/news/2018-03-20/china-deploys-ai-cameras-to-tackle-jaywalkers-in-shenzhen/9567430 (viewed 23 March 2018).
[80] Identity Bill, s 9.
[81] Identity Bill, s 10.
[82] Identity Bill, s 10(2).
[83] Explanatory Memorandum to the Identity Bill, 24 [140]-[142].
[84] Explanatory Memorandum to the Identity Bill, 25 [145].
[85] Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), [58]. Available at https://rm.coe.int/16806840ba (viewed 20 March 2018).

[86] Intergovernmental Agreement on Identity Matching Services (5 October 2017), 15 [5.4]. Available at https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf (viewed 26 March 2018).
[87] Mr Holger Haibach, Rapporteur to the Council of Europe Parliamentary Assembly, Explanatory Memorandum to *The need for a global consideration of the human rights implications of biometrics*, COE Doc 12522 (16 February 2011), 8. Available at http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=13103 (viewed 28 March 2018).
[88] https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx (viewed 20 March 2018).
[89] https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Face-verification-service.aspx (viewed 20 March 2018).
[90] This is plain on the face of the Bill, but confirmed in the Explanatory Memorandum to the Identity Bill, 10 [29].
[91] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill,54-55.
[92] Identity Bill, s 12.
[93] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill,, 53.
[94] Identity Bill, s 7(2).
[95] Explanatory Memorandum to the Identity Bill,, 2 [4].
[96] Explanatory Memorandum to the Identity Bill,28 [173].
[97] Explanatory Memorandum to the Identity Bill,28 [173].
[98] *Road Transport (Driver Licensing) Regulation 2017* (NSW), reg 10.
[99] *Road Transport (Driver Licensing) Regulation 2017* (NSW), reg 100, *Road Transport Act 2013* (NSW), s 56.
[100] *Road Transport (Driver Licensing) Regulation 2017* (NSW), reg 100(2).
[101] *Australian Passports Act 2005* (Cth), s 42.
[102] Australian Passports Determination 2015 (Cth), cl 20(1).
[103] *Australian Passports Act 2005* (Cth), s 43(1); Australian Passports Determination 2015 (Cth), cl 21(1).
[104] Australian Passports Determination 2015 (Cth), 20(3).
[105] *Migration Act 1958* (Cth), ss 5A(1), 257A.
[106] *Migration Act* 1958 (Cth), s 5A(1)(g).
[107] *Migration Act* 1958 (Cth), ss 257A, 166, 170, 175.
[108] *Migration Act* 1958 (Cth), ss 261AA, 261AE.
[109] See Identity Bill, s 5(1)(j)(iii).
[110] See Identity Bill, s 5(1)(l).
[111] See Identity Bill, s 5(1)(k).
[112] See Identity Bill, s 5(1)(m).
[113] NSW Department of Transport — Road and Marine Services website, http://www.rms.nsw.gov.au/about/corporate-publications/statistics/registrationandlicensing/tables/table211.html (viewed 23 March 2018).
[114] Australian Bureau of Statistics website, http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0 (viewed 23 March 2018).
[115] Australian Bureau of Statistics website, http://www.abs.gov.au/ausstats/abs@.nsf/Previousproducts/3235.0Main%20Features152014?opendocument&tabname=Summary&prodno=3235.0&issue=2014&num=&view= (viewed 23 March 2018).
[116] Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40(1) *University of New South Wales Law Journal* (Advance), 8. Available at http://www7.austlii.edu.au/cgi-bin/download.cgi/au/journals/UNSWLJ/2017/6 (viewed 23 March 2018).
[117]Australian Bureau of Statistics website, http://www.abs.gov.au/ausstats/abs@.nsf/0/E92EA270A32AF8F1CA256953007D9AFA?Opendocument (viewed 23 March 2018).
[118] Australian Bureau of Statistics website, http://www.abs.gov.au/ausstats/abs@.nsf/products/961B6B53B87C130ACA2574030010BD05 (viewed 25 March 2018).
[119] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill, 46.
[120] Clayton Utz, *Document Verification Service: National Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS* (31 March 2015), 8. Available at

https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/PIAReportAExpandedPrivateSector.pdf (viewed 28 March 2018).

[121] Clayton Utz, *Document Verification Service: National Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS* (31 March 2015), 10. Available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/PIAReportAExpandedPrivateSector.pdf (viewed 28 March 2018).

[122] Intergovernmental Agreement on Identify-Matching Services (5 October 2017), 5. Available at https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf (viewed 26 March 2018).

[123] Attorney-General's Department, *Identity Crime and Misuse in Australia 2016*, 53. Available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx (viewed 28 March 2018).

[124] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill, 46-47.

[125] Fee Schedule in Addendum 1 to Clayton Utz, *Document Verification Service: National Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS* (31 March 2015), 8. Available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/PIAReportAExpandedPrivateSector.pdf (viewed 28 March 2018).

[126] Statement of Compatibility with Human Rights, in Attachment A to the Explanatory Memorandum to the Identity Bill, 46-47.

[127] Attorney-General's Department, Template *Memorandum of Understanding — Services — For Participation as a Data Holding Agency in the National Facial Biometric Capability — Version 5.0* (10 October 2016), Schedule 4, available at https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Data-holding-agency-services-mou-template-fvs.pdf (viewed 23 March 2018).

[128] Proposed s 56A of the *Australian Passports Act* 2005 (Cth). See cl 3 of Schedule 1 of the Passports Bill.

[129] Explanatory Memorandum to the Passports Bill,2 [5].

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

REVIEW OF THE IDENTITY-MATCHING SERVICES BILL 2018 AND THE AUSTRALIAN PASSPORTS AMENDMENT (IDENTITY-MATCHING SERVICES) BILL 2018

Questions on Notice

1. Senator David Fawcett asked the following question at the hearing on 3 May 2018:

a) **Senator FAWCETT:** [Y]ou raised concerns about the security of data, if there was a concentration of data in a hub. Are you aware of any standard of security that would satisfy your concerns in that regard or just on principle do you think that's a risk that is unacceptable? As I took it from your statement, you were almost indicating it was an unacceptable risk to have that much data held in the one place.

The answer to the senator's question is:

a) With respect to the question of the risks associated with the aggregation of data, the Commission refers to the response to the senator's question given in evidence at the hearing by Commissioner Santow. The aggregation of large amounts of personal information in a single system carries significant risks. Claims that this aggregation is necessary to achieve a legitimate purpose, and that the consequent risks are proportionate to achieving that purpose, must be closely scrutinised and substantiated with compelling evidence. As noted in the Commission's written submission, international bodies have stated that alternative technical solutions to the creation of centralised databases be implemented wherever feasible. In any event, where personal information is aggregated, either by way of a centralised database such as the NDLFRS or via a 'hub', very stringent protections must be put in place to ensure that risks of unauthorised access to, or theft of, personal information are minimised. Necessary protections include: ensuring that only a minimum amount of personal information is retained in and accessible through the relevant database or system; controlling carefully who, and in what circumstances, the information may be accessed; as well as ensuring that the highest standard of technical data-protection systems is implemented. The Commission does not possess technical expertise in relation to particular standards of data security.

2. The Hon. Mark Dreyfus QC, MP asked the following question at the hearing on 3 May 2018:

a) **Mr DREYFUS:** Can you tell me which Commonwealth department administers this document verification services?

The answer to the honourable member's question is:

a) In evidence given later in the Committee's hearing on 3 May 2018, a representative of the Department of Home Affairs confirmed that that department now administers the document verification service.