Submission to the 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

Joint Submission by Drs Kate Galloway, Monique Mann and Jake Goldenfien on behalf of FutureWise and the Australian Privacy Foundation.

Australian
Privacy
Foundation

1. Introduction

Thank you for the opportunity to make a submission on the Identity-matching Services Bill 2018 ('Bill'). This submission is on behalf of and jointly authored by Future Wise and the Australian Privacy Foundation:

Future Wise is a group of Australian professionals of varied backgrounds who seek to promote ideas which improve the long-term direction of Australia, particularly in the areas of technology, health and education. More information about FutureWise is available on our website.[1]

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. More information about The Australian Privacy Foundation is available on our website.[2]

We are willing to provide further clarification of any of the points in the submission, or for one of the authors to attend the hearing in person if required.

2. Summary of Recommendations

1. The Bill must be rejected because as it is framed, it fails to represent a legitimate or proportionate response to the challenges articulated in the Explanatory Memorandum.
2. The Bill enables the collection, storage and processing of sensitive biometric information of individuals who have not been convicted of criminal offences by the Department of Home Affairs. The storage of such information by policing agencies absent a conviction has been found to violate rights to private life in other jurisdictions.[3] The use of this data by the Department of Home Affairs is permitted for various policing purposes, however data governance processes and structures applicable to that Department remain unclear. The scope of data collection, storage and processing by the Department of Home Affairs requires strict specification and limitation before this level of data collection can be considered legitimate.
3. Government culture and processes overall require an overhaul before enacting further information architecture such as that included in the Bill.

If the Committee is not persuaded of this position, we urge the Committee, at a bare minimum, to take up the following recommendations:

4. Urgent policy consideration is required to address human rights and regulatory shortcomings in Australia's biometric information collection and sharing regime. A re-evaluation of privacy protections and law enforcement exemptions to them, is also required.
5. The nature of the data sharing activities within the Bill must be narrowed to represent legitimacy or proportionality that would justify the information architecture established by the Bill.

---

[1] <https://www.futurewise.org.au>.
[2] <https://privacy.org.au/>.
[3] *S and Marper v United Kingdom* [2008] ECHR 1581.

6. The extent of law enforcement activities contemplated by the Bill must be significantly curtailed to reflect only those activities of an urgent nature involving significant and imminent risk to public safety.
7. The Bill must differentiate between law enforcement activities requiring simple identity checks, those requiring a biometric component, and those requiring facial recognition.
8. The Bill must limit the circumstances by which one-to-many searching of databases or image sources (including web-scraping, for example of social media sites, and Closed Circuit Television ['CCTV']) can be conducted. This is not required in order to meet the Bill's stated objectives.
9. The Bill must not draw within its information architecture the activities of local government and non-government entities, including CCTV networks, without at the very least, further clarifying the basis on which identity verification is core to the activities of those entities rather than being imposed by law enforcement requirements.
10. The Bill must recognise even information sharing through a 'hub' as integral to the information infrastructure of data analytics perfomed by the Department of Home Affairs, and bring such activities within the overarching protections contemplated in this submission.
11. The proposals in the Bill require the addition of governance infrastructure that at a bare minimum, supports ongoing input of citizen representatives into the operation of the proposals, and affords individuals with rights against the abuse or misuse of their data.
12. Biometric databases, and access to them, should be periodically reviewed and information about them should be made publicly available. In order for this to occur additional oversight mechanisms are necessary. Greater oversight arrangements, such the Biometrics Commissioner model that has been adopted in the United Kingdom, are required.

3. Background

Facial recognition systems digitise, store and compare facial templates that measure the position of facial features and can be used to conduct one-to-one matching to verify identity, or one-to-many searching of databases or image sources to identify unknown persons. In late 2015 the Commonwealth government announced a national facial recognition system—the National Facial Biometric Matching Capability or simply 'The Capability'—would be implemented. This system uses existing identification documents, such as licences and passports, to extract and share biometric information between state, territory and national government databases.

The Parliamentary Joint Committee on Intelligence and Security has commenced a review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018.

- The Identity-matching Services Bill 2018 will authorise the Department of Home Affairs to collect, use and disclose identification information in order to operate the systems that will support a set of new biometric face-matching services.
- The Australian Passports Amendment (Identity-matching Services) Bill 2018 will authorise the Minister for Foreign Affairs to disclose personal information for the purpose of participating in a service to share or match information relating to the identity of a person.

The Explanatory Memoranda acknowledge that the Bills respond legislatively to activities already sanctioned under COAG agreements as discussed above. To the extent that existing activities are brought within legislative purview, with attendant proposed accountability mechanisms—such as audit and reporting requirements—the Bills go some way to addressing concerns about the introduction through administrative procedures, of biometric sharing.[4] However a number of issues and concerns remain, and are the subject of this submission which focuses principally on the Identity-matching Services Bill 2018 ('Bill'), with additional comments on the Australian Passports Amendment (Identity-matching Services) Bill 2018.

4. Outline of concerns

The Bill is intended to facilitate sharing of citizens' biometric data between jurisdictions for law enforcement and other identification purposes. The Explanatory Memorandum seeks to establish the legitimacy and proportionality of this sharing by claiming:

1. Identity theft is increasing.
2. Law enforcement requires an efficient, fast, and accurate means of ascertaining individuals' identity to protect society, including through preventing and prosecuting identity theft.
3. Doing so necessarily requires biometric data.
4. Jurisdictional limits inhibit all jurisdictions from carrying out their law enforcement efficiently, and from successfully protecting society.

[4] See, eg, 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* 121, 127.

5. The Commonwealth will facilitate states sharing biometric data through a 'hub'.
6. The hub does not collect or store data and so is, effectively, simply an interface and neutral in terms of citizens' privacy.
7. States seeking to share and access data must have a lawful excuse for doing so—derived from existing laws.

Despite bringing the proposals to parliamentary scrutiny, there remain significant issues of concern regarding the approach outlined in the Explanatory Memorandum and the Bill:

1. The justification for the proposal is not coherent, failing to establish, except through direct assertion, that the proposed measures are a legitimate and proportionate [5] government incursion into citizens' privacy. There is no evidence that this system will indeed achieve the goal of preventing identity theft (or by extension community protection, community safety and road safety) as outlined in the Explanatory Memorandum. There is a complete absence of evidence that this system will improve national security or is required in order to do so.
2. The Bill is couched in terms of community protection, and community safety,[6] and even road safety, to justify the proposal—yet these terms are defined so widely as to potentially draw almost all activities within the Bill's ambit. The effect is that the biometric matching might be deployed for almost any purpose without limit. For instance, those purposes likely enable the collection and processing of data by the Department of Home Affairs for criminal intelligence profiling.
3. The Commonwealth declares its role in the Identity Data Sharing Service ('IDSS') to be limited to providing a 'hub', facilitating the sharing of data that is already held by governments, merely transmitting data rather than collecting or storing it.[7] It thus purports to embed effective privacy processes. The IDSS, together with the other data matching processes, cannot be interpreted alone in the data landscape. To do so ignores the role of data linkages in upscaling government capacity to erode citizens' privacy.[8] All processes under the Bill comprise the tools of big data in the hands of government, with limited oversight only.
4. The Bill lacks a governance process beyond an annual report to the Minister, to be tabled in Parliament.[9]

The remainder of the submission discusses these areas in more detail.

5. Justification for the proposal within the Bill

While the purpose of the Bill is to:

[5] Mere assertions of legitimacy appear throughout the Explanatory Memorandum for the Identity-matching Services Bill 2018 eg:
[6] See, eg, Identity-matching Services Bill 2018, s 17(2)(a). 'Community safety' is defined in s6(6) and 'road safety' in s6(7).
[7] Explanatory Memorandum, 56.
[8] Recognised, eg, in Information Integrity Solutions, *National Facial Biometric Matching Capability Privacy Impact Assessment – Interoperability Hub,* for Attorney -General's Department (August 2015) ('*Privacy Impact Assessment'*), 5.
[9] See, eg, recommendations in Mann and Smith, above n 3; ibid.

> facilitate the secure, automated and accountable exchange of identity information between the Commonwealth and state and territory governments[10]

This purpose in turn seeks to facilitate 'community and identity verification activities',[11] namely:

- Preventing identity crime
- General law enforcement
- National security
- Protective security
- Community safety
- Road safety, and
- Identity verification

The Explanatory Memorandum outlines a range of justifications for providing biometric matching services in pursuit of these goals, including:

- enhancing national security, combating crime and increasing service delivery opportunities [7]
- strengthening the integrity and security of Australia's identity infrastructure [8]
- streamlining identification of unknown persons, and detecting people using multiple fraudulent identities [12]
- making government and private sector services more accessible and convenient to citizens [13]
- (perhaps) benefiting victims of natural disasters who have lost identity documents [14]
- making it harder for persons to avoid traffic fines, demerit points or licence cancellations by acquiring a false driver licence [15]

While it may be that the proposal will achieve these goals, these instances either:

a) do not warrant the extent of privacy invasion ushered in by the proposal (eg catching traffic fine avoiders, or 'to detect and remove duplicate records or to detect and replace poor quality photographic images'[12]); or

b) fail to articulate how a data matching scheme will achieve the stated objective (eg 'preventing' identity fraud[13]); or

c) can be achieved by a scheme that does not involve *facial* data matching and would therefore be less invasive.[14]

---

[10] Explanatory Memorandum, clause 1.
[11] Bill, long title; also defined in s6.
[12] Explanatory Memorandum, [120].
[13] Explanatory Memorandum, [63].
[14] For an explanation about the enhanced invasiveness of facial recognition, see Mann and Smith, above n 3.

A. Disproportionate invasion of privacy

The 'general' law enforcement goals of the Bill encompass everything from detecting terrorism to drivers' licence infringement. In expressing such a broad application, the Bill undermines its own case for proportionality of the measures. There appears to be no need, for example, to expose all Australian citizens to biometric data matching to remove duplicate records. It is incumbent on government to design other methods of record management that do not involve significant privacy incursions.

Further, 'mak[ing] it harder for individuals to avoid traffic fines'[15] does not warrant the establishment of a national biometric matching facility that sweeps up the data of all Australian citizens.

The Explanatory Memorandum identifies 'efficiency' as a key justification for the powers in the Bill.[16] In the first instance, 'efficiency' relates to 'assess[ing] the nature of a potential threat'. Duplication of records, or identification of poorer quality facial images does not constitute the kind of threat that might normally justify privacy intrusion.

Subsequently, the Explanatory Memorandum identifies the IDSS as an 'efficient' means of facilitating the transfer of biometric information between agencies. Yet according to the Explanatory Memorandum, this does not involve 'any facial biometric or other data-matching'.[17] On this argument, efficiency might therefore be achieved in the absence of the more intrusive aspects of the proposal (though see below for analysis of the IDSS).

The extent of the law enforcement activities contemplated by the Bill should therefore be re-examined, to be limited to those absolutely necessary for public safety—rather than those that are simply convenient or 'efficient'.

Australia is out of step with international precedent[18] that has established the collection and retention of sensitive biometric information of those who have not been convicted of a criminal offence is a violation of the right to private life. Biometric information is sensitive information and should only be collected with the consent of the individual concerned.

In the *Marper* decision, the ECHR found in favour of the applicants, stating that:

> ... the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.[19]

To the extent that the Bill effectively establishes a type of policing role for the Department of Home Affairs, the concerns raised in *Marper* resonate.

---

[15] Explanatory Memorandum, 53.
[16] See, eg, Explanatory Memorandum, 50, 54-6.
[17] Ibid 54.
[18] *S and Marper v United Kingdom* [2008] ECHR 1581 ('*Marper*').
[19] Ibid.

B. Data matching irrelevant to achieving objectives

The Explanatory Memorandum seeks to justify the proposal to a large extent, through establishing 'identity crime' as a significant contemporary law enforcement—and community safety—problem. It then claims that the proposal will prevent such crime.[20]

At the very least, a claim that the proposal will necessarily 'prevent' identity crime is overstated. For example, a significant arena of identity crime occurs online through poor online security either at the institutional or user end, through human error, or through unlawful activity unrelated to biometric data.[21] In none of these circumstances will the exchange or matching of biometric data—either one-to-one or one-to-many—'prevent' the crime.

Similarly, the claim is made that the OPOLS (One Person One Licence) Service will 'deter' dangerous driving. While a worthy law enforcement goal, there is no evidence that the holding of one licence, through the operation of national biometric data exchange, will do any such thing. Indeed, as illustrated through a recent tragic case in Queensland, dangerous driving will occur regardless of licensing requirements.[22]

In another use case, the Explanatory Memorandum claims that the Bill will protect the community against risks through

> identifying a person where there are reasonable grounds to believe the person is acting suspiciously in the vicinity of a crowded public place and who may be planning an act involving harm to the public.[23]

In such circumstances, identity is not relevant to prevention of any risk and this fails to justify the proposal.

Many of the use cases cited to justify the Bill fail to establish how data matching will achieve the objectives, or they overstate the case. The activities contemplated by the Bill should therefore be narrowed only to those activities that are genuinely able to achieve the objectives. In particular, one-to-many matching (or the identification of unknown persons via their facial templates) is not required to achieve these objectives and the Bill must limit the circumstances in which this can occur.

C. Facial data not necessary

There are other use cases that might appear to support the need for law enforcement to access identity data, but which can be achieved without the use of biometric data. These include

---

[20] Ibid [8], [63], [73], [75], 58.
[21] See, eg, Attorney General's Department, 'Identity Crime and Misuse in Australia 2016' (Commonwealth of Australia, 2016). For examples of the Australian government failing to protect citizens' data, see, eg: Nick Whigham, 'Parts of ATO website up and running as agency tries to recover lost data' *News.Com* (14 December 2016) http://www news.com.au/technology/online/parts-of-ato-website-up-and-running-as-agency-tries-to-recover-lost-data/news-story/0719d4ac98d794ad3618e8f058b49bf2>; Paul Farrell, 'The Medicare machine: patient details of 'any Australian' for sale on darknet' *the Guardian* (4 July 2017) <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet>; 'Census: Australian Bureau of Statistics says website attacked by overseas hackers' *ABC Online* (10 August 2016) <http://www.abc.net.au/news/2016-08-10/australian-bureau-of-statistics-says-census-website-hacked/7712216>.
[22] Christine Flatley, '"Terrible" driver denied bail over Christmas Day deaths' *Canberra Times* (7 March 2018) <http://www.canberratimes.com.au/queensland/terrible-driver-denied-bail-over-christmas-day-deaths-20180307-p4z38b.html>.
[23] Explanatory Memorandum, 94.

identifying deceased persons.[24] First, there is no guarantee that the features of a deceased person might be recognised through biometric data. Secondly, if the technology may be useful, the imperative for identification—where other means are available—does not present the urgency that would justify intruding on the privacy of all Australians.

Additionally, a significant amount of identity fraud occurs online. As fraudsters do not generally appear in person online, such fraud is unlikely to warrant biometric data matching.

To this extent, the scope of the Bill's operation should be wound back to encompass only those activities that present a genuine legitimate, proportionate case for the application of the technology.

Further, the technology introduces a series of other concerns. For example, there is the potential for error—both false positives and false negatives. The accuracy of face recognition technology varies under various conditions (controlled and uncontrolled). There is also the potential for racial discrimination and bias in these systems. There is the potential for mis-matching and no avenues for review or appeal of decision.

6. **Scope of Bill supports 'function creep'**

Individuals who consented to providing a photograph to obtain a license or a passport did not consent to their facial templates being extracted from that image to be used for law enforcement, security, intelligence or other purposes. This Bill *already represents unacceptable scope creep* where information collected for one purpose is being used for secondary purposes beyond the scope or conditions supporting its original collection. The individual who provided information—in this case their photographic image—is not aware of, and thus has not consented to, any further secondary or tertiary uses.

In addition, the Bill's community protection function—separately defined, but in fact reliant upon and therefore part of identity matching overall—is so broadly defined as to contemplate, or justify, almost any government activity. Further, the examples cited of potential application of the data matching, span pre-emptive action against terrorists, to fine defaulters, to enforcing money laundering laws, to finding missing persons, and identifying those engaging in 'suspicious' activities at major events.

The Explanatory Memorandum asserts that the Facial Identification Service ('FIS')[25] contains more stringent restrictions than other processes, claiming:

> 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.[26]

It points to the example of the community safety purpose of 'identifying individuals at risk of, or who have suffered, physical harm, or individuals who are *reasonably believed* to be involved with a *significant risk* to public health or safety',[27] there must be a 'reasonable belief' that the person is a 'significant risk' to public health or safety. Further, it states that:

---

[24] Ibid.
[25] A 'one-to-many' identification system, comparing an individual's face with faces from a database.
[26] Explanatory Memorandum, 51 (emphasis added).
[27] Ibid (emphasis added). See Bill, s6(6)(b).

> *It is not intended*, for example, to allow for widespread scanning of CCTV footage in public places or at major events for example (sic).[28]

Using this example diverts the reader from the overall point of the risk associated with the proposed legislative framework. In the first place, the FIS can still be used for all of the other—very broad—purposes. Secondly, there is no 'additional' protection with FIS—the purposes of its application are the same as other processes dealt with in the Bill. Finally, while it may not 'be intended' to allow for scanning of data outside the contemplated government databases, the hub—central to the operations contemplated by the Bill—establishes the information infrastructure to accommodate such information in the future.

The Explanatory Memorandum is, in this sense, misleading as to the nature and effect of the proposal, and therefore diverts consideration away from effective governance structures other than stipulating broad fields of law enforcement endeavour.

The Bill provides for local government and non-government entities to be brought within the scheme. These provisions effectively position such entities as agents of law enforcement for the purpose of identity verification. This is said to be justified because:

> Through their day-to-day service delivery activities, local government authorities and non-government entities handle a significant volume of identification documents for the purpose of verifying identity.[29]

The Bill further justifies local government and non-government service providers participate in identity verification on the basis that they do so with the consent of the individual, and that identity verification is reasonably necessary for the provision of the service. These are flawed assumptions for two reasons.

First, consent does not represent choice. As local government or non-government entities will be required by law to verify identity according to the processes in the Bill, the individual's choice is limited to using the relevant service, or not. Refusing to consent to the verification processes will presumably mean that the individual cannot access the service. Where these services are essential (such as Council services, or banking) individuals will have no real choice but to consent. This aspect of the Bill therefore effectively brings all citizens within the provisions of the legislation. Such scope places a disproportionate invasion of privacy on the citizen, relative to the goals of the Bill.

Secondly, the Explanatory Memorandum contradicts its own justification. On the one hand, it claims that local government and non-government entities play a 'significant role in detecting the use of stolen or fraudulent identification documents and fighting identity crime' and that this is why they 'must have access to the fast and secure face-matching provided by the FVS.'[30] This seems to indicate a primary role of fighting identity crime. Yet the next paragraph identifies that part of the protection for individuals is that identity verification must be 'reasonably necessary for [the entities'] functions or activities'. On this reading, service delivery is the primary role. The use case is made on the basis that such front-line organisations have access to face-matching facilities to achieve the objectives of the Bill—not in furtherance of their own service delivery.

Further, it is observed that the use case for non-government entities engaging in identity verification draws on government requirements that they do so. Where government can demand that local government or non-government entities verify identity, it makes identity

---

[28] Ibid (emphasis added).
[29] Explanatory Memorandum, 48.
[30] Ibid.

verification 'reasonably necessary' to those entities' operation. This is a circular argument, whereby government can generate its own use case beyond the legitimate and proportionate need for the proposed data matching.

The ostensible prioritisation of crime fighting in the Bill's justification, over genuine operational reasons for identity verification, exposes the government's true intent as to the scope of data at its disposal. These provisions represent the inevitable function creep of the proposals, expanding the expressed scope of data sharing by law enforcement bodies, to include local government *and even* non-government entities as law enforcement proxies.

This aspect of the legislation is opportunistic, expanding the available data-set exponentially in what is a disproportionate and illegitimate incursion on citizens' privacy. It should be rejected and the Bill should introduce limits in relation to one-to-many matching via Closed Circuit Television (CCTV) and other data sources, such as information gleaned from the internet (for example social media).

7. An information 'hub' does make incursions into citizens' data ('IDSS')

The Explanatory Memorandum states that the IDSS is a 'hub' only, and that

> The service will not involve any facial biometric or other data matching, but will merely transmit identification information from one participating entity to another.[31]

This understates the effect of the IDSS in a 'big data' context. Providing a hub facilitates the applications of big data analytics, as all data transmitted through the hub *may* be stored by the Department of Home Affairs (although in the context of IDSS such storage is not necessary). While the 'hub' operates on a query and response model for service-users, it collects and aggregates data for the database controllers. Describing the 'hub' as just a singular instance of data exchange is misleading because it fails to describe the scale of data gathering and processing by the Department of Home Affairs that the 'hub' interface facilitates. Data collection by the Department of Home Affairs from other government agencies and private entities through the 'hub' will generate an extraordinarily large aggregation of personal data for the sake of high-level analytics by the Department of Home Affairs. Similarly, data sharing between agencies through the IDSS may become an element of analyticsm operations for other agencies. This qualitatively different data environment/infrastructure opens new avenues for the dissembling and restructuring of citizens' data. The policing and intelligence remit of the Department of Home Affairs remains murky, and such large-scale analytics and insight generation could have significant consequences for more highly policed groups such as activists, migrants and refugees.

8. Additional governance required

Governance under the Bill includes:

- retaining metadata concerning the operation of the facilities to enable reporting
- annual reporting to Parliament
- requirements for law enforcement agencies to derive their own lawful reason for accessing data
- greater specification and justification for data collection and use by the Department of Home Affairs

[31] Ibid [30].

- training
- high level access only
- compliance with the *Privacy Act*

Despite these features, the Bill fails to enlist more substantive information governance as has been recommended elsewhere, such as:

- strengthening the functions and funding of the Office of the Australian Information Commissioner ('OAIC');
- establishing a Biometrics Commissioner should be introduced[32]

Increased oversight and regulation by independent statutory commissioners may have an ability to respond to concerns related to consent, retention and use of biometric information. Of note, the *Privacy Impact Assessment* suggested that overall governance of such a system is more important that governance at individual agency level.[33] Further, there is no structure that engages with civil society representatives, provides for complaint procedures and review, or engages expressly with a broad view of privacy.[34]

Further, compliance with the *Privacy Act 1988* (Cth) is meaningless in this context due to the significant carve outs for law enforcement agencies and agencies with a law enforcement function. Under the *Privacy Act 1988* (Cth), sensitive information includes biometric information and templates. Sensitive information must only be collected with the consent of the individual concerned, *unless the entity is an enforcement body and there is a reasonable belief that the information is necessary to the entity's functions*. Entities cannot use or disclose information collected for a particular purpose for a secondary purpose without the consent of the individual, *unless the information is reasonably necessary for one or more enforcement related activities*. These exemptions are significant as enforcement agencies or agencies with an enforcement function do not need consent, a warrant, or a court order to collect and retain photographs or other forms of biometric information, to process this information to create facial templates and disclose or share this information with other agencies for the purpose of data matching. Given this, a re-evaluation of privacy protections and law enforcement exemptions to them, is urgently required.

The Bill should not be accepted until appropriate governance structures are incorporated into the design of the facilities.

9. General observations

This submission does not accept that government in Australia, or Australian laws, are sufficiently equipped to protect citizens' data privacy. This is particularly the case for the proposals in the Bill, which engage not only with data collection and sharing, but deal with *sensitive* data and data matching. This is an emerging field with known and unknown risks to the citizen including:

- false positives arising from facial recognition technologies
- invasion of privacy of individuals who have no relationship with any incident
- substantial evidence of a lack of suitable culture of data governance within government

[32] Mann and Smith, above n 3, 122.
[33] *Privacy Impact Assessment*, above n 8, 5.
[34] Ibid.

- scope creep

Establishing data infrastructure that fails to engage adequately with risk to the citizen is enticing for government but sets the foundation for erosion of the rule of law. This principle establishes the boundary between the legitimate exercise of government power and the freedom of the citizen.

Facial recognition is highly privacy invasive. It provides a gateway connecting an individual's presence in physical space to information stored in large and ever-expanding databases held by government, law enforcement and security agencies. Photographs (and facial templates) from data rich environments such as social media can be mined and integrated into big data. It can be conducted from a distance and can be integrated with existing surveillance systems such as CCTV enabling tracking through public places. We are on our way to automated and real-time surveillance of public spaces. Further, it is likely that this system will reveal more about an individual than just their identity.

Considerable developments have occurred in the roll out of national facial recognition databases and urgent policy consideration is required to address human rights and regulatory shortcomings. Until the scope of the proposal is adequately constrained with reference to the circumstances of deployment, and the governance structures that promote the rights of citizens, this Bill should be rejected.