



AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

6 December 2018

PO Box A147

Sydney South

NSW 1235

DX 585 Sydney

www.alhr.org.au

Dennis Richardson AO
Reviewer
Comprehensive Review
c/o Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By email: comprehensivereview@ag.gov.au

Dear Sir

Comprehensive review of the legal framework governing the National Intelligence Community

Australian Lawyers for Human Rights (**ALHR**) is grateful for the opportunity to provide this submission in relation to the Comprehensive Review (**the Review**).

ALHR

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

Table of Contents

1.	Summary	3
2	ALHR’s Concerns	6
3	Applying a human rights framework.....	8
	Part A: Problems with Substantive Legislation.....	9
4	Overview	9
5	Excessive Penalties.....	11
6.	Overreach and Vagueness	13
7	Lack of whistleblower and public interest protections.....	15
	Part B: Problems common to Substantive legislation and Legislative Framework	15
8	Impractical or counterproductive	15
9.	Risk of Error, risk of loss and need to support integrity of data	17
10	Examples	21
11.	Lack of Oversight.....	23
12.	Weakness of Australian Privacy Legislation	24
13	Conclusion.....	29
	Appendix: Recent legislation which has impinged upon Australians’ human rights in the name of national security (or proposes to do so)	30

... the more capable the intelligence and law enforcement agencies become, the more robust the governance and oversight mechanisms have to be.¹

[The] literature suggests that current accountability and oversight mechanisms have been reduced over time, and are inadequate for intelligence practices.²

1. Summary

- 1.1 As mentioned on the home webpage for this Review,³ the previous 2017 Independent Intelligence Review (**2017 Review**) recommended:

A comprehensive review of the Acts governing Australia's intelligence community ... to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians.

- 1.2 **We submit that the best legislative framework would be one which aligns relevant legislation with community values and which reflects a risk-based system whereby stronger regulation is placed around those intelligence community activities which pose a higher risk of infringement of human rights.**⁴ Such a framework would enable the key criteria of accountability, transparency and fairness, and encourage public trust. It would impact as little as possible on the human rights of persons subject to the legislation.
- 1.3 We submit that in order for the Review to be truly comprehensive, not only the **legislative framework** needs to be considered, but also the **substantive legislation** which is the 'interface' through which Australians interact with the national intelligence community.
- 1.4 Without fully understanding the substantive legislation which describes the extent to which, and the context within which, Australians human rights and the rule of law are impacted by increasingly severe national security legislation, we submit that the Review cannot make appropriate decisions in relation to the best overall national intelligence structure. As the Data to Decisions Cooperative Research Centre says, in the context of national security, 'legislation cannot be viewed in isolation from other regulatory elements and cultural influences.'⁵
- 1.5 Indeed it may be most appropriate to consider the substance of the activities of the Australian intelligence community first of all, and then envisage an organic framework of laws and accountability mechanisms around those capabilities which will assist in the aim of driving good decision-making, rather than the 'landscape that's just a massive mess' that is said to exist at present.⁶
- 1.6 Substantive legislation can empower and assist intelligence organisations (as in the case of the data retention legislation) and can also lay down penalties for national security offences. It is the

¹ Survey participant, quoted in *Big Data Technology and National Security Report*, Data to Decisions Cooperative Research Centre, June 2018, p 81, at https://www.d2dcrc.com.au/m/u/2018/08/30/australia-report-june-2018_O8RxnPu.pdf, speaking about the need to strengthen privacy legislation in Australia in the national intelligence context. The interviews on which the report is based were conducted in 2015 and the report relates to the law as at 31 March 2016, therefore the report does not entirely reflect the current legal landscape.

² *Methodology Report - Big Data Technology and National Security*, Data to Decisions Cooperative Research Centre, June 2018, p 22, at <https://www.d2dcrc.com.au/m/u/2018/08/30/method-report-june-2018.pdf>, citing *Australian and NSW Government, Martin Place Siege Joint Commonwealth – New South Wales Review*, January 2015.

³ <https://www.ag.gov.au/NationalSecurity/Pages/Comprehensive-review-of-the-legal-framework-governing-the-national-intelligence-community.aspx>

⁴ Data to Decisions Cooperative Research Centre, op cit (footnote 1), p 85.

⁵ Data to Decisions Cooperative Research Centre, op cit, p 7.

⁶ Survey participant, Data to Decisions Cooperative Research Centre, op cit, p 120.

substantive legislation that would generally contain protections for the rights of Australians, such as privacy, public interest and whistleblower protections, rather than the framework or 'structural' legislation, although some legislation does both: - that is, it establishes the framework of the particular intelligence organisation as well as laying down the more substantive rules for its operation, and penalties for breach of the legislation.

- 1.7 The substantive legislation that empowers intelligence organisations generally involves collection of personal data and related breaches of privacy rights. That legislation needs to be viewed in the context of the weaknesses in existing Australian privacy legislation which are discussed further at section 12. While it is heartening to read the findings of the 2018 Report from the Data to Decisions Cooperative Research Centre as to the generally strong privacy culture within the national intelligence community, it is also disheartening to find that:
- because most intelligence organisations are exempt from the Australian Privacy Act, they have little guidance from legislation, relying largely on internal manuals, and sometimes not understanding the relevant legislation;⁷
 - generally, threshold access levels for individuals' personal data are set very low and legislation is silent on what can happen to the data after it has been accessed.⁸
- 1.8 An increased focus in respect of 'national security' in Australia in recent decades has involved a departure from previous review and public transparency standards. Australian legislation has authorised the interception of non-suspects' communication,⁹ allowed the Attorney General to issue warrants on the application of ASIO's Director General,¹⁰ introduced a new regime allowing the government to intercept 'stored communications' – that is, communications sent across a telecommunications system and accessible to the intended recipient;¹¹ and allowed the Director-General of ASIO to apply to the Attorney-General for questioning and detention warrants.¹²
- 1.9 Effectively, Australia has:
- moved from largely relying on Australia's criminal law (with all its tested procedural safeguards) in promoting national security, to relying on a system that uses special provisions to target classes of people that may include innocent bystanders;¹³
 - moved from allowing judges to authorise the interception of communications to and from a telecommunications service in specific circumstances –where there were reasonable grounds for suspecting that a particular person was likely to use the service, and the information obtained was likely to assist the investigation of an offence in which the person involved - to a system that allows elected officials to issue such warrants on the ASIO Director-General's application;
 - expanded the scope of communications that the Government could monitor for the purposes of national security protection; and

⁷ In the words of one survey participant: "There seems to be a lot of folklore and myth about what you're allowed to do and not allowed to do. Often when you actually say no show me the legislation, it's actually quite different to what people had assumed it to be. So there's a lot of hubris around what the constraints are. They're often not nearly as strict as what people are led to believe." (Data to Decision Cooperative Research Centre, op cit, p 118).

⁸ These issues raised in the 2018 Report are discussed further below.

⁹ *Telecommunications (Interception) Amendment Act 2006* (Cth) sections 9 and 46.

¹⁰ *Ibid*, section 9(1).

¹¹ *Ibid*, section 110.

¹² *Australian Security Intelligence Organisation Act 1979* (Cth) Part III div III.

¹³ David Hume and George Williams, 'Who's Listening? Intercepting the telephone calls, emails and SMSs of innocent people' (2006) 31 *Alternative Law Journal*, 211; Kent Roach, *The 9/11 Effect: Comparative Counter-terrorism* (Cambridge University Press, 2011) 317; George Williams, 'A Decade of Australian Anti-terror Laws' (2011) 35 *Melbourne University Law Review* 1137; 1140; and George Williams, 'One year On: Australia's Legal Response to September 11' (2002) *Alternative Law Journal* 212.

- included non-suspects within the class of persons numerous government and semi-government bodies could monitor.

1.10 The substantive legislation which penalises national security offences:

- is often deliberately vague, lacking crucial core definitions,
- through amendments in recent years has demonstrated an increasing tendency to redefine commonly used terms to give them a completely different meaning, and
- is often complex,

all of which make it very **difficult for people to understand whether they might be committing an offence or not**.

1.11 This is a significant problem in the light of the **excessive penalties** which apply for breach of national security legislation, often irrespective of whether or not any harm has been caused, and often contrary to the Commonwealth's own Guidelines in relation to the imposition of penalties (see section 5 below).

1.12 It is also a significant problem in the context of the current dysfunctionality of the Administrative Appeals Tribunal, as reported in the *Saturday Paper*.¹⁴

1.13 Definitions are inconsistent between different pieces of legislation, not just in relation to key terms such as 'record' or 'data', but even in relation to the categorisation of law enforcement agencies. This makes consistency of approach between agencies and understanding of legislation even more difficult.¹⁵

1.14 Moreover, it is of concern that, without concerted advocacy by civil society in Australia, problems such as those referred to above might not have been addressed at all prior to the passage of much recent substantive legislation relating to national security. The parliamentary committee process (which provides a very important mechanism for detailed scrutiny of legislation) is increasingly offering shorter and shorter time frames - sometimes as little as five working days - for receipt of submissions from civil society, experts, stakeholders and interested members of the community. This, coupled with national security legislation that is poorly drafted or overbroad constitutes a significant threat to human rights, the rule of law and democracy in Australia.

1.15 Issues which are relevant both to the legislative framework and to the substantive legislation include:

- the **impracticality or counterproductive nature** of some 'national security' legislation;
- the **inherent risks of misinterpretation and biased analysis** occurring in relation to personal information gathered under the wider powers being granted to national security agencies under recent legislation, with profound reputational and legal impact. This has consequences for the **ability of Ministers to delegate decisions to computer programmes**, which is a trend that particularly concerns us;
- the **lack of Parliamentary and court oversight**, as to which we support, with some minor exceptions, the amendments proposed by Senator Patrick in the *Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018*. We agree with Senator Patrick that 'While Australia's intelligence community has grown rapidly over the past two decades, the mechanisms of accountability and review overseeing those agencies have received much less attention, resources and authority' and that existing restrictions upon PJCS oversight should generally be removed.¹⁶ We note that exemptions

¹⁴ Mike Secombe, "Political stacking leaves appeals tribunal in chaos", *The Saturday Paper*, 25 November 2018, <https://www.thesaturdaypaper.com.au/news/politics/2018/11/24/political-stacking-leaves-appeals-tribunal-chaos/15429780007187>

¹⁵ Data to Decisions Cooperative Research Centre, op cit, pp 169-170 and 172.

¹⁶ Second Reading Speech xxx

from Parliamentary and court oversight are built into much of the recent substantive legislation, for example the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, and submit that these exemptions should be removed;

- **the weakness of Australian privacy legislation**, particularly in comparison to European legislation, which contains numerous exemptions. We note that exemptions from the Commonwealth *Privacy Act* are built into much of the recent substantive legislation.

1.16 Issues relevant to the legislative framework include:

- the combining of so many different portfolios into the **Home Affairs ‘mega Ministry’** which removes previous practical checks and balances which support Australians’ rights and appears to entrench, rather than improve, existing failings (see generally the Audit Report in relation to *the Integration of the Department of Immigration and Border Protection and the Australian Customs and Border Protection Service*.¹⁷)
- the lack of public interest and whistleblower protections; and
- the general lack of public, parliamentary and legislative oversight.

1.17 We note that the Inspector-General comments at page 3 of her submission in relation to Senator Patrick’s Bill that ‘the overarching purpose of the IGIS’s activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, *and respects human rights*’ (emphasis added).

1.18 We submit that using a human rights framework to test the issues to be considered by the Review is both a useful and essential process which will assist in the appropriate balancing of the competing rights and interests involved. This is discussed further below in section 3.

1.19 Given the enormous breadth of the scope of the Review, it is not possible for us to do more than provide an outline in relation to some of the issues noted in this submission, which draws upon some of the submissions we have made to the Commonwealth government over the past few years. We would be happy to expand on any of these issues orally or in writing if requested.

2 ALHR’s Concerns

*It is no exaggeration to suggest that the current swathe of proposed laws risk placing Australia, not merely on a police state footing, but a garrisoned footing. Terrorism, for all its fearful properties, remains an idea, a tactic and a method. The consequences of responding to it are quite something else. Shredding civil liberties is the first step to admitting a failure in dealing with the very problem a society should resist.*¹⁸

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

2.2 ALHR endorses the views of the Parliamentary Joint Committee on Human Rights (PJCHR) expressed in Guidance Note 1 of December 2014¹⁹ as to the nature of Australia’s human, civil and

¹⁷ <https://www.anao.gov.au/work/performance-audit/integration-department-immigration-and-border-protection-and-australian-customs-and-border>

¹⁸ “Winding back the Liberties: The New Anti-Terror Laws in Australia,” 25 September 2014, Rule of Law Institute website, accessed 28 September 2014, <http://www.ruleoflaw.org.au/anti-terror-laws-in-australia/>

¹⁹ Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, *Guidance Note 1: Drafting*

- political rights obligations, and agrees that the inclusion of human rights ‘safeguards’ in Commonwealth legislation is directly relevant to Australia’s compliance with those obligations.
- 2.3 Australia is a contracting party to the ICCPR which was signed by the Australian government on 18 December 1972 and ratified on 13 August 1980. Pursuant to Article 26 of the 1969 Vienna Convention on the Law of Treaties, Australia has an obligation to the international community to implement, uphold, protect and respect all of the rights contained in the ICCPR.
 - 2.4 Generally, behaviour should not be protected by Australian law where that behaviour itself infringes other human rights. There is no hierarchy of human rights – they are all interrelated, interdependent and indivisible. Where protection is desired for particular behaviour it will be relevant to what extent that behaviour reflects respect for the rights of others.
 - 2.5 It is only through holding all behaviours up to the standard of international human rights that one can help improve and reform harmful and discriminatory practices.
 - 2.6 **Legislation should represent an appropriate and proportionate response to the problems and harms being dealt with by the legislation, and adherence to international human rights law and standards is an important indicator of proportionality.**²⁰
 - 2.7 We note that the proportionality test is contained in the privacy guidelines for ASIO and other agencies²¹, and therefore this type of framework is not unknown to the national intelligence community.²² As the Data to Decisions Cooperative Research Centre notes, relevant considerations include weighing factors such as the scope and objectives of the collector, the purpose of the collection, the seriousness of the issue, the availability of less intrusive measures to achieve similar ends, and whether an interference with fundamental rights and freedoms is involved.²³ We submit that the human rights framework we propose is very similar but has the advantage of providing a theoretical underpinning and further guidelines for the way in which competing interests should be balanced. However in applying the framework, it is important that the negative impacts of any breach of human rights are fully taken into account and not merely paid lip service when balanced against undefined and unexplained ‘national security’ interests, as is too often the case with recent Australian legislation.
 - 2.8 The Data to Decisions Cooperative Research Centre notes that there appears to be no publicly-available test for national intelligence analysts to use in order to balance national security purposes against adverse risks to the privacy and rights of data subjects, despite the ‘profound legal, reputational and commercial implications for subjects of the assessment’. The Centre recommends that such a test be introduced, as well as a requirement to apply the test, so as to ensure public trust in the fairness of the analytical process.²⁴
 - 2.9 The Centre also recommends the further articulation of the proportionality assessment approach and its harmonisation across all law enforcement and national security organisations as a

Statements of Compatibility, December 2014, available at http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources, see also previous *Practice Note 1* which was replaced by the Guidance Note, available at <https://www.humanrights.gov.au/parliamentary-joint-committee-human-rights>.

²⁰ See generally Law Council of Australia, “*Anti-Terrorism Reform Project*” October 2013, <http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/a-z-docs/Oct%202013%20Update%20-%20Anti-Terrorism%20Reform%20Project.pdf> and par 1.6.1 ‘Proportionality Test’ in Data to Decisions Cooperative Research Centre, op cit, p 14, and see the discussion at p 142 and ff, particularly p 146

²¹ Data to Decisions Cooperative Research Centre, op cit, p 153 and ff

²² Data to Decisions Cooperative Research Centre, op cit, p 149 and ff.

²³ Data to Decisions Cooperative Research Centre, op cit, p 142.

²⁴ Data to Decisions Cooperative Research Centre, op cit, p 155.

‘rigorous general framework that could be adapted for decision-makers at different levels’.²⁵ In that regard we recommend the human rights framework described below.

3 Applying a human rights framework

The balancing of indivisible and interdependent human rights

- 3.1 What happens where national security matters (such as the collection and retention of information for national security purposes) impinges on the human rights, including privacy rights of Australians? International human rights law has developed a process or set of principles by which such conflicts can be managed, both within the realm of human rights alone and in relation to external issues.

Rights must be balanced where they conflict

- 3.2 In general terms, no human right ‘trumps’ any other right – all are equally valuable (the principle of indivisibility) and should be protected together (the principle of interdependence).
- 3.3 Some rights are expressed as absolutes, such as the right to be free from slavery, torture, cruel or inhuman or degrading punishment or treatment, or arbitrary deprivation of life, and the right to recognition as a person in law.²⁶
- 3.4 Subject to those absolutes, all rights must be **balanced** where they conflict so as to maximise the practice of other rights to the greatest possible extent, in ‘an atmosphere of mutual consideration’²⁷ and so as to ‘ensure that none is inappropriately sacrificed’.²⁸ This is sometimes described as a process of providing **reasonable accommodation** to other rights and other persons: ‘a fair balance needs to be struck between the rights of the individual and the rights of others.’²⁹ This is similar to the test of proportionate response to the harm in question which is generally used to assess whether or not legislation is too wide in its scope.

Taking account of context and other values

- 3.5 The balancing and reasonable accommodation tests are very much dependent upon context and cannot be used in the abstract. They may also need to call upon other rights and other values (such as reasonableness or proportionality), which is particularly relevant in the context of national security.
- 3.6 Human rights can validly be restricted if the restriction is prescribed by law and is necessary for the protection of public safety, public health or morals or for the protection of the rights and freedoms of others.

The good faith of those seeking State protection

- 3.7 Human rights entail **both rights and obligations**. **Where protection is desired for particular behaviour it will be relevant to what extent that behaviour reflects respect for the rights of others**. Generally, behaviour should not be protected by Australian law where that behaviour itself infringes other human rights, and substantive evidence that national security legislation is only infringing human rights to the minimum extent possible should be provided, not just stated.

²⁵ Data to Decisions Cooperative Research Centre, op cit, p 168 and see further at section 4.2.2, p 223.

²⁶ See generally Attorney-General’s Department Public Sector Guidance Sheet: *Absolute rights* at <https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/Absoluterights.aspx>

²⁷ Grimm, op cit, 2382.

²⁸ Donald and Howard, op cit, p i.

²⁹ Donald and Howard, op cit, p i.

- 3.8 In balancing the competing claims, it is important to minimise any negative impact; to impinge as little as possible upon other rights. Therefore it will be very important to consider whether national security legislation unreasonably impacts upon Australians.
- 3.9 That is, where there is a conflict between human rights and other interests it may be necessary to limit or constrain the other interests if they are to be implemented in a way that limits the free exercise of human rights.

Six key principles

- 3.10 Former Australian Human Rights and Equal Opportunity Commissioner The Hon John Von Doussa QC recommends³⁰ that the balancing process between human rights and national security be carried out in accordance with the following six principles, with which we concur:
- (1) Do not violate non-derogable human rights (rights that should not be suspended, even in an emergency, being the ‘absolute’ rights referred to above, as well as the right to life and the right to freedom of thought, conscience and religion (Article 4(2) of the *International Covenant on Civil and Political Rights*³¹).
 - (2) Other rights should only be infringed in accordance with human rights law;
 - (3) Respect the role of an independent judiciary;
 - (4) Establish regular, independent review of the operation of counter-terrorism laws;
 - (5) Make sure persons who are subject to counter-terrorism laws can challenge the validity of decisions that impact on their rights; and
 - (6) Introduce stronger human rights protections.³²
- 3.11 We understand that key stakeholders in the intelligence community “appreciate ... that the goal cannot be to simply remove all impediments to the ‘flow of intelligence.’ ...[but] rather to re-consider existing rules in view of new technological capacities, to ensure that rights are appropriately balanced.”³³

Part A: Problems with Substantive Legislation

4 Overview

- 4.1 It is submitted that much recent Australian national security legislation is generally overbroad, substantially encouraging the increased surveillance of innocent Australians not suspected of any crime, and severely compromising their personal privacy and digital rights (see generally, *State of Digital Rights Report*, Digital Rights Watch, 2018).³⁴ The restructuring of numerous federal government Departments into one multi-layered mega-Ministry which has also taken on areas of work from other Departments, such as the Attorney-General’s Department, provides the structure to support this significant change in policing direction. ALHR does not support the

³⁰ “Incorporating Human Rights Principles Into National Security Measures“, speech to *International Conference On Terrorism, Human Security And Development: Human Rights Perspectives*, City University of Hong Kong, 16-17 October 2007 at <https://www.humanrights.gov.au/news/speeches/incorporating-human-rights-principles-national-security-measures>

³¹ See generally Attorney-General’s Department Public Sector Guidance Sheet: *Absolute rights* at <https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/Absoluterights.aspx>

³² Details of these recommendations are set out at: <https://www.humanrights.gov.au/news/speeches/incorporating-human-rights-principles-national-security-measures>

³³ *Big Data Technology and National Security*, Data to Decisions Cooperative Research Centre, June 2018, at https://www.d2drcr.com.au/m/u/2018/08/30/australia-report-june-2018_O8RxnPu.pdf

³⁴ Digital Rights Watch, 2018, at <https://digitalrightswatch.org.au/2018/05/14/the-state-of-digital-rights/>.

increased infringement by government of Australians' privacy rights and endorses calls by Digital Rights Watch and others for increased accountability and transparency (subject to secrecy about operational capabilities such as investigative techniques or analytical approaches)³⁵ in relation to the collection, retention and use by governments and commercial interests of personal metadata, with independent oversight officers and agencies. We submit that such measures will reduce the information gap between intelligence community users of personal information and the public,³⁶ and thus enhance public trust of government activities.

- 4.2 Recent legislation relating to national security regularly contains excessive penalties even where no harm has occurred, with inappropriately narrow exemptions which ignore the benefits of whistleblowing and public interest concerns. Such legislation is often vague and lacking in crucial definitions. These problems are mutually re-enforcing, resulting in draconian legislation with severe penalties but which is hard to understand and apply.
- 4.3 ALHR endorses the concerns of the Law Council that individuals "just will not know where the boundaries are in terms of whether or not they're actually committing criminal offences".³⁷ This situation is inconsistent with the rule of law which requires that the law is capable of being known to everyone, so that everyone can comply.
- 4.4 A related problem is that when lack of clarity in legislation is drawn to the attention of government committees, the response of committees is often to amend the relevant Explanatory Memorandum (which does not have legal force) rather than to correct the legislation itself. This does not provide an appropriate legal solution, particularly given that it is not possible for courts to give advisory opinions on legislation which is difficult to interpret.
- 4.5 In this section we take as examples the recent 'foreign interference' package of legislation comprising the *Foreign Influence Transparency Scheme Act 2018 (FITS)*, *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* and the *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017*.
- 4.6 All the pieces of legislation in the 'foreign interference' package share some common faults, including:
- (1) Excessive penalties, even where no harm has occurred;
 - (2) Lack of crucial definitions ('espionage,' 'sabotage,' 'political violence,' 'foreign interference,' 'prejudice Australia's national security', 'an Australian democratic or political right or duty') and re-definition of normal terminology to mean something different than usual ('on behalf of' means not only where an agent acts for a principal but where the first person knows or might know that the second person is going to undertake a particular activity - not necessarily even involving the first person);³⁸
 - (3) Excessively narrow exemptions, including in relation to whistleblowing, and a lack of public interest exemptions or defences;
 - (4) Unexamined assumptions about foreign influence/ lack of evidence for the approach taken, and related failure to adopt a risk-based approach; and
 - (5) Disregard for impact on the rule of law, individual human rights, freedom of political discourse and hence disregard for the negative legislative impact on Australia's democracy.

³⁵ See Data to Decisions Cooperative Research Centre, op cit, p 111 ff.

³⁶ See Data to Decisions Cooperative Research Centre, op cit, p 117 ff.

³⁷ President of the Law Council of Australia, Hansard, Parliamentary Joint Committee on Intelligence and Security, 16 March 2018, p 10.

³⁸ This would have been the effect of the original section 11(3) of FITS: "... a person undertakes an activity on behalf of a foreign principal if both the person and the foreign principal knew or expected that:(a) the person would or might undertake the activity".

4.7 We discuss some of these points further below.

5 Excessive Penalties

- 5.1 Much recent legislation relating to national security issues including the ‘foreign interference’ package imposes excessive penalties irrespective of whether or not any harm was caused (and whether or not the activity took place).
- 5.2 **Such legislation, which might result in incarceration for non-malignant behaviour which actually causes no harm, is potentially in breach of Article 9 of the ICCPR and Article 3 of the Universal Declaration of Human Rights (UDHR) which protect the right to liberty.**
- 5.3 The *Foreign Influence Transparency Scheme Act (FITS)* is not about covert influence, as has been acknowledged many times, as opposed to the *National Security Legislation Amendment (Espionage and Foreign Interference) Act* which is (at least in part) about covert influence. FITS deals with perfectly ordinary and - if not for the Act - lawful behaviour. As the Attorney General’s Department has said:
- *“a key purpose of the Foreign Influence Transparency Scheme has been to shed light on quite legitimate dealings that are not criminal.”*³⁹
 - *“it is not the covert Foreign Influence Transparency Scheme... There is no inference or suggestion in the Foreign Influence Transparency Scheme that that foreign influence is harmful.”*⁴⁰
 - *“there is no intention to cast negative aspersions or to criminalise or to otherwise take the view that it is wrong for there to be foreign influence; it’s simply that there is value in that being disclosed and it being transparent to the community and decision-makers”*⁴¹
- 5.4 That is, the only potential malfeasance relates to a new obligation created by the Act: the failure of the relevant person to register with the regulator, with its consequent obligations. The Commonwealth Government’s own Guidelines⁴² provide that such matters as ‘whether the conduct in some way so seriously contravenes fundamental values as to be harmful to society’ should be considered before imposing criminal penalties.⁴³ The Guidelines quote Report 95 of the Australian Law Reform Commission: *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, to the effect that:

*The main purposes of criminal law are traditionally considered to be deterrence and punishment. Central to the concept of criminality are the notion of individual culpability and the criminal intention for one’s actions.*⁴⁴

and that

*... a key characteristic of a crime, as opposed to other forms of prohibited behaviour, is the repugnance attached to the act, which invokes social censure and shame.*⁴⁵

³⁹ Hansard, Joint Committee evidence 16 March 2018, p 49.

⁴⁰ Hansard, Joint Committee evidence 16 March 2018, p 54.

⁴¹ Hansard, Joint Committee evidence 16 March 2018, p 53.

⁴² Most recent version dated 2011 is available at:

<https://www.ag.gov.au/Publications/Pages/GuidetoFramingCommonwealthOffencesInfringementNoticesandEnforcementPowers.aspx>

⁴³ Ibid, page 13.

⁴⁴ Australian Law Reform Commission, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, Report 95: 2003, available at <http://www.austlii.edu.au/au/other/alrc/publications/reports/95/>, quoted at page 12.

⁴⁵ ALRC 95 at 2.9, quoted at page 12.

- 5.5 ALHR was particularly concerned to read comments from the Attorney General’s Department to the effect that criminal prosecution would be used sparingly – but should be retained, effectively in order to encourage people to register under the Act. It was said that:

“in relation to that compliance and the suggestion that there is [a] negative connotation that comes from criminal proceedings—absolutely there is. But what I would say in respect of that registration piece is that the scheme has been designed to support compliance with the scheme, and hence that ability to engage with somebody who ought to be registered and to formally engage with them— we could of course do so informally prior—and to flag: ‘It appears to us from what we see that you are engaging in activity of this nature. This seems to us to be something that requires registration. It wouldn’t proceed directly to criminal action. Again, if there’s an inadvertent failure to comply, the first port of call would not be criminal sanctions.’”⁴⁶

- 5.6 If it is indeed the case that the Attorney General’s Department does not propose to apply criminal sanctions in the manner contemplated in the legislation, then criminal penalties should not apply for what is admitted to be otherwise legal behaviour. It would appear that the imposition of criminal penalties is being used to ‘encourage’ citizens to register under the FITS Act, which we submit is clearly inconsistent with the Commonwealth Guidelines and amounts to an abuse of the rule of law. We note that under section 15B of the *Crimes Act 1914* (Cwlth), where a criminal penalty involves more than 6 months imprisonment, no limitation period applies and a person can be prosecuted at any later time.
- 5.7 The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* also imposes excessive penalties of up to 25 years imprisonment upon people who ‘deal’ with certain information even if they do not reveal it but only copy, possess or receive the information. We refer to detailed comments on the various versions of Bill made by the Human Rights Law Centre concerning these provisions.⁴⁷
- 5.8 We are concerned that a similar situation applies under the *National Security Legislation Amendment (Espionage and Foreign Interference) Act*, both in relation to the reliance that persons potentially caught by the legislation will need to place on the good graces of the Attorney General at the time, and in relation to the uncertainties as to whether or not the legislation applies. Similar comments have been made in relation to this legislation, to the effect that the Attorney General would exercise discretion as to whether or not persons would be prosecuted for espionage if they communicated with the United Nations and that communication might be argued to prejudice Australia’s national security. However at the same time, the Attorney General’s Department has said that “Ultimately, enforcement of the offences will be a matter for the AFP.”⁴⁸
- 5.9 There appears to be an emerging trend whereby the Federal Government:
- legislates to impose disproportionately severe penalties (described as ‘horrific over-reach’⁴⁹), without allowing any ‘public benefit,’ public domain or ‘whistleblower’ defences, for a wide range of matters;

⁴⁶ Hansard, Joint Committee evidence 16 March 2018, pp 54 – 55.

⁴⁷ Submissions 11, 11.1 and 11.2 at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/EspionageFI/nterference/Submissions

⁴⁸ Hansard, Joint Committee evidence 16 March 2018, p 55.

⁴⁹ Michael Bradley, ‘What Brandis won’t tell us about S35P’, ABC at <<http://www.abc.net.au/news/2014-11-06/bradley-what-brandis-wont-tell-us-about-s35p/5871684>> accessed 9 November 2014 and see Simon Breheny, ‘George Brandis’s Solution A Cure Worse than the Disease’, *Institute of Public Affairs Website* at <<http://ipa.org.au/news/3198/george-brandis%27s-solution-a-cure-worse-than-the-disease>> accessed 9 November 2014, being a reproduction of an article originally published in *The Australian* on 7th November 2014.

but then

- states publicly that the government is unlikely to encourage prosecutions under the legislation against certain classes of person - as it has done in the context of disclosure by journalists of security operations.⁵⁰

5.10 **How can one have confidence that Commonwealth prosecution guidelines will be correctly applied, given that many offences, such as those in the *National Security Legislation Amendment (Espionage and Foreign Interference) Act* and the *Foreign Influence Transparency Scheme Act* do not appear to be framed in accordance with the Commonwealth's *Guide to Framing Commonwealth Offences*?**

6. Overreach and Vagueness

"... our laws are too complex, all of them are too verbose, they're unbelievably over-sophisticated ... law needs to be completely accessible to anyone with goodwill and a modicum of intelligence ... [C]ounter-terrorism is the great example – [it's] let's enact a whole lot of law, unbelievably sophisticated law, and we do. I don't know if you feel safer against terrorists because ... we've got all those bits in the criminal code. I don't. We already had really good laws against murder."⁵¹

- 6.1 Overreach in national security legislation always risks being counterproductive, as discussed further in section 7. The 'foreign interference' package of legislation is a good recent example of confusing and overbroad legislation which makes it hard for Australians to know whether or not they are complying with the law and which we submit is therefore inconsistent with fundamental rule of law principles.

For example, under the FITS Act as originally drafted, it appeared likely that:

- Australian academics working in consultation with overseas Universities or lecturing abroad would be forced to register as 'foreign agents' (with associated reporting and notification obligations) purely because of their academic collaboration with a foreign organisation;
- Calling your mother in New Zealand to say that you were going on a demonstration in Melbourne in support of refugees could also have required registration – whether or not you actually went to the demonstration!

While it was said that the legislation was not intended to have these effects, it was certainly drafted so broadly that such outcomes were possible.⁵² The final wording of the Act is somewhat narrower, but anomalies do remain.

- 6.2 The lack of definitions in these laws relating to crucial elements of 'national security' is also a particular problem. The Head of ASIO has expressed the view that 'national security' may cover any type of 'threat', saying that:

the definition of 'national security' is something that does actually change through time. We've always sought to redefine it as circumstances in the world change. I don't think it's unreasonable at all to include, on occasions when there is a direct nexus between the two issues you raised, which is political or economic international activity and national security. That seems to me to be very, very defensible. One needs to be careful. You can't just sort of lay it down and say, 'That is national security.' It's a very elusive definition. It depends on what is actually a threat to the nation at any given time. And if something is a threat, then I consider that to be part of national security, and it's part of my remit to identify those

⁵⁰ Bradley, op cit;

⁵¹ Survey participant, Data to Decisions Cooperative Research Centre, op cit, p 79.

⁵² ALHR Submission 7, par 6.17, p 12, accessible at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TransparencySchemeBill/Submissions

*threats and reflect them to the government, to provide early advice on the threat as it presents.*⁵³

- 6.3 Given that ‘foreign interference’ is not defined, the inclusion of ‘foreign interference’ as one type of national security activity is problematic, as again it is difficult for a person to know if this element of a crime is made out.
- 6.4 ALHR submits that it is **not appropriate for criminal liability to be based on overly broad and potentially changing meanings**. To include economic relations or interests as national security matters is unworkably vague and will have an unreasonably chilling impact on freedom of speech and discourse regarding matters of genuine public interest. This is inconsistent with democratic principles. Although in practice a number of non-intelligence and non-military issues may have an impact on a country’s national security – such as food security, climatic conditions, economic inequality and energy security, for example – this is no reason to criminalise holding or dealing with information about such matters, as would appear to be the effect of the Act. It is also virtually impossible for the man in the street to evaluate what might or might not be an action which damages Australia’s economic relations with another country, particularly given the tendency for regimes worldwide to respond economically by raising tariffs or similar as a response to perceived disrespect or political slights.
- 6.5 There is no defence for harming or causing ‘prejudice to’ or ‘interference with’ national security, **even in relation to issues that are matters of public discussion**. All terms are excessively broad and vague and make it very hard to know what is required of people seeking to comply with the legislation. Comprehensibility of the elements of a crime, including the ability to clearly distinguish different elements of the offence, is crucial but is not established by these laws.
- 6.6 The Chair of the committee that developed the Criminal Code, Dr Neal, says that the Code is meant to be based on simple and uniform concepts, but “there is nothing simple about these concepts,” (in the ‘foreign interference’ legislation), the breadth of which is “just unworkable”.⁵⁴ “Do we want to go that far?” he asks.⁵⁵
- 6.7 Similar confusion is demonstrated in the new Criminal Code sections 92.2 and 92.3 (Offence of Intentional Foreign interference and Offence of reckless foreign interference) introduced under the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*. Subsection (3) of each section says that the actor/ ‘agent’ committing ‘foreign interference’ by interfering with a ‘target’ “does not need to have in mind a particular foreign principal”; and “may have in mind more than one foreign principal”. The target does not have to be a politician or government member. It can be anybody exercising any ‘Australian democratic or political right or duty’ (not defined) or the target can be a ‘political or government process.’ However under subsection (2) of each of the sections, it is a criminal offence not to reveal to the ‘target’ the existence of the foreign principal on whose behalf the actor is meant to be trying to influence the target. How can the actor reveal this if they don’t know who the foreign principal is? And how can the actor reveal anything to a ‘target’ which is a process and not a person?
- 6.8 ALHR endorses the concerns expressed by Amnesty International in the *Sydney Morning Herald*¹³ that under the changes to the Criminal Code, as introduced by the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*, it is possible that normal activities of human rights organisations, such as sharing information with UN bodies, could amount to crimes under section 91.2 if the relevant information has the potential to embarrass the government and thus perhaps to ‘prejudice’ Australia’s national security interests. It is extraordinary that communication with the public international organisations which form part of our international rules-based order should be potentially criminalised in this manner.

⁵³ Hansard, Joint Committee evidence 16 March 2018, p 44.

⁵⁴ Hansard, Parliamentary Joint Committee on Intelligence and Security, 16 March 2018, p 10.

⁵⁵ Hansard, Parliamentary Joint Committee on Intelligence and Security, 16 March 2018, p 13.

- 6.9 While ALHR recognises that it has now been clarified that mere embarrassment will not be sufficient to establish harm to Australia’s national security, given the very broad definition of national security it will be very difficult for organisations and individuals to assess whether or not their actions might be caught by section 91.2. We again reiterate that such an uncertain legislative outcome is inconsistent with the rule of law.

7 Lack of whistleblower and public interest protections

- 7.1 In the light of the excessive penalties involved in most ‘national security’ legislation, difficulty in comprehending many elements of relevant offences, and the general secrecy and lack of transparency as to how that legislation operates in practice, it is very clear that public interest and whistleblower protections are essential to the fair operation of Australian intelligence legislation and to public trust in our national intelligence system. Unfortunately, such exemptions are generally lacking and where they exist are very limited in scope.
- 7.2 We submit that such protections should be included in all national security legislation, including the ‘foreign interference’ package, especially where the disclosure relates to significant misconduct or behaviour which is otherwise unlawful. We note that since 2014 ASIO officers have been immune from all criminal and civil liability for conduct in the course of a “special intelligence operation” which is an additional matter of concern and an additional reason why whistleblower and public interest protections are needed.⁵⁶

Part B: Problems common to Substantive legislation and Legislative Framework

Research participants identified a broad range of groups who may be subject to the risks associated with Big Data. In particular, the most common answer to the question, [‘]who was exposed to risks[?’], was ‘everyone.’⁵⁷

8 Impractical or counterproductive

- 8.1 The recent murder in Bourke Street, Melbourne carried out by a man whose passport had been withdrawn because he posed a terrorist threat raised questions about the desirability of oversight for Australian intelligence services⁵⁸ but also about the extent to which data trawling appears to have replaced community policing, even for those listed as being potentially dangerous.
- 8.2 Many argue that internal terrorism is more effectively prevented through community policing⁵⁹ than through data collection which simply makes the ‘haystack’ (or silos) larger. As one US headline put it: “NSA Whistleblower: Government Failed to Stop Boston Bombing Because It Was Overwhelmed with Data from Mass Surveillance On Americans.”⁶⁰ Similarly Australian intelligence personnel have reported being overwhelmed by the sheer mass of data:

... we’re seizing more than terabytes now when we do warrants. So the Big Data issue is becoming bigger and one job we did recently ... there was so much information ... that we physically did not have the assets in Australia to download it quick enough to start to look at it. So we literally had to [send] terabytes of data over to the US for them to crunch it for us.

⁵⁶ See generally Submission No 2 of Gilbert and Tobin, 2014, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/National_Security_Amendment_Bill_2014/Submissions

⁵⁷ Data to Decisions Cooperative Research Centre, op cit, p 217.

⁵⁸ Bernard Keane, “It’s time for real oversight on intelligence and counter-terrorism”, Crikey 12 November 2018 at <https://www.crikey.com.au/2018/11/12/bourke-street-oversight-intelligence/>

⁵⁹ Ben Taub, “The Spy Who Came Home: Why an expert in counterterrorism became a beat cop”, *The New Yorker*, 1 May 2018, at <https://www.newyorker.com/magazine/2018/05/07/the-spy-who-came-home>

⁶⁰ Washington’s Blog, 1 November 2013, at <https://washingtonsblog.com/2013/11/nsa-whistleblower-government-failed-to-stop-boston-bombing-because-it-was-overwhelmed-with-data-from-mass-surveillance-on-americans.html>

*So the problem we had when we started this is getting bigger because the amount of data we're seizing is definitely increasing.*⁶¹

- 8.3 That is, it is dubious whether the push for intense surveillance of Australians' movements, images and metadata which has occurred in recent years through legislation such as that listed in the **Appendix to this Submission** is likely to be practical and to achieve the claimed results, despite involving enormous infringements upon Australians' privacy, freedom of assembly, free speech and civil rights generally. As one survey participant puts it:

*... be careful about access to material. If you don't have the ability to analyse it properly then you're better off not having it to be quite frank...*⁶²

- 8.4 Even with the protection of recent legislation, which it is submitted has a marked tendency to empower government agencies at the expense of citizens' personal privacy, contrary to community expectations, intelligence agencies still face practical problems as well as the erosion of public trust engendered by a secretive system.
- 8.5 **Practical difficulties** include cultural problems with information-sharing between Australian intelligence organisations, such as turf protection, resulting in the Australian Government Investigation Standards not being followed,⁶³ and technological problems, whereby even within the one organisation different data-gathering measures and legacy systems result in disparate data sets that cannot all be aggregated or interrogated together⁶⁴ and inter-agency sharing is very difficult because "most law enforcement agencies within Australia have completely different ways of dealing with data and formatting and storing information."⁶⁵ It remains to be seen whether the merging of various Departments and organisations within Home Affairs will solve such problems. The recent Audit Report in relation to the *Integration of the Department of Immigration and Border Protection and the Australian Customs and Border Protection Service* expressed concern as to various record-keeping and other inefficiencies in the Home Affairs Department.⁶⁶
- 8.6 **Data security** also remains a practical problem. As the Data to Decisions Cooperative Research Centre, notes, 'Big Data' systems 'may have a large surface of exposure, impact on more people, and have many facets which all need to be effectively protected', all of which issues present further challenges 'where the system is intended to be accessed and used by a large number of individuals in different agencies and different geographic locations.'⁶⁷ In the words of one survey participant:
- ... one of the key challenges is securing the data. So amassing greater quantities of data, drawing greater linkages and storing that data all creates a higher risk of that data being attractive to criminal elements and others.*⁶⁸
- 8.7 And while there may be some benefits in amalgamating so many Departments and organisations into Home Affairs, it certainly makes them all more vulnerable to external infiltration.
- 8.8 For a government data system to be trustworthy, points out one survey participant, people need to feel that they can understand how their data is used, that the system is transparent, and that

⁶¹ *Big Data Technology and National Security*, Data to Decisions Cooperative Research Centre, June 2018, p 30, and see section 2.4 at page 36ff, at https://www.d2drc.com.au/m/u/2018/08/30/australia-report-june-2018_O8RxnPu.pdf

⁶² Data to Decisions Cooperative Research Centre, op cit, p 58.

⁶³ Data to Decisions Cooperative Research Centre, op cit, pp 32 and 35.

⁶⁴ Data to Decisions Cooperative Research Centre, op cit, pp 49 and 50.

⁶⁵ Data to Decisions Cooperative Research Centre, op cit, p 97.

⁶⁶ <https://www.anao.gov.au/work/performance-audit/integration-department-immigration-and-border-protection-and-australian-customs-and-border>

⁶⁷ Data to Decisions Cooperative Research Centre, op cit, p 177 -179.

⁶⁸ Data to Decisions Cooperative Research Centre, op cit, p 56.

they can influence the system⁶⁹. Another notes that there is no excuse for unauthorised access to peoples' personal data and there need to be both disciplinary and criminal offences for such abuse for 'corrupt or malevolent official use'⁷⁰ – as well as a reasonably high legal access threshold. As one survey participant said:

"... one of the premises of the Privacy Act is about people having control over their personal information and an understanding of why it's being collected and how it's being used. Although the power relationship is often unbalanced in terms of people being asked to provide their personal information in order to get a service or in order to interact with government, nonetheless one of the safeguards is the transparency part of the equation. So then, if it's the used for unintended purposes that has the potential to undermine community trust and confidence."⁷¹

- 8.9 Survey participants also noted that there is little legislative guidance around the use of data once it is collected – the discussions being focused on which agencies could access the data but not on what might happen after an agency is given access.⁷²
- 8.10 In this context, another indicator of transparency and proportionality would be a **statutory requirement for data to be deleted when it is no longer relevant**. Most of the legislation under consideration contains no such practical requirement.⁷³ We submit that such a requirement should be included in the *Identity-Matching Services Bill 2018* and the *Australian Passports Amendment (Identity-Matching Services) Bill 2018 in relation to the identification information provided by third parties to the Commonwealth 'hub' for comparison purposes*. As one survey participant suggested in another context, reference to relevant material could still be kept ('the person's identity was confirmed as being consistent with the information provided by the bank') without the actual data having to be retained.⁷⁴
- 8.11 **None of these criteria is met at present.**

9. Risk of Error, risk of loss and need to support integrity of data

Inherent problems in predictive analytics

- 9.1 As the Data to Decisions Cooperative Research Centre notes, "predictive analytics based on unreliable data carry... an inherent risk of personal information being misinterpreted; assessed out of context' erroneously weighted; or unfairly dealt with in some other way."⁷⁵ There is an inherent risk in relation to data system errors that adversely impact individuals in a national security context where the individual is not aware of the issue and is unable to correct any error. False or inaccurate assessments will continue to be retained in relevant data systems. Even something as simple as data-matching of car number plates has demonstrated systemic errors.⁷⁶ **Data integrity in gathering and assessing intelligence material is essential in order to achieve public trust**. While some regard has been paid to the overview of collection mechanisms, little regard has been had to the necessity of monitoring of data analysis.⁷⁷

⁶⁹ Data to Decisions Cooperative Research Centre, op cit, p 48.

⁷⁰ Data to Decisions Cooperative Research Centre, op cit, p 54.

⁷¹ Data to Decisions Cooperative Research Centre, op cit, p 54.

⁷² Data to Decisions Cooperative Research Centre, op cit, p 84.

⁷³ Data to Decisions Cooperative Research Centre, op cit, p 67 and see p 166 ff.

⁷⁴ Data to Decisions Cooperative Research Centre, op cit, p 78.

⁷⁵ Data to Decisions Cooperative Research Centre, op cit, pp 155 and 156.

⁷⁶ Data to Decisions Cooperative Research Centre, op cit, p 156, referring to Victorian experiences.

⁷⁷ Data to Decisions Cooperative Research Centre, op cit, p 194.

- 9.2 The following comments are relevant to the issue of error impacting on a person’s human rights in the context of predictive analytics, whether used for national security purposes by a data analyst or used by a computer to which a Minister has delegated some decision⁷⁸.
- 9.3 ALHR notes that the ability of Ministers to delegate decisions to computer programmes is already well entrenched in legislation,⁷⁹ as is the ability of all parts of government to use computer programmes to assist in decisions on day to day matters, even including important issues such as risk assessments of refugee claims.
- 9.4 The problem is of course that a computer programme is only as good as the programme design and the information put into it. ‘Algorithmic bias,’ it is noted, ‘is now a widely studied problem that refers to how human biases creep into the decisions made by computers. The problem has led to gendered language translations, biased criminal sentencing recommendations, and racially skewed facial recognition systems.’⁸⁰ Studies in the US have already found evidence of bias in facial recognition, bail and sentencing decisions, law enforcement decision-making, online advertising and recruiting, all driven by purportedly neutral algorithms.⁸¹ Edwards and Veale observe that algorithmic systems trained on past biased data which introduce correlations based on race, religion, gender, sexuality, or disability without careful consideration are inherently likely to recreate or even exacerbate discrimination seen in past decision-making.⁸² A risk of resultant incorrect, unfair or arbitrary decisions is therefore very real.⁸³
- 9.5 Further, computer programmes are unlikely to be coded by persons who understand how to interpret the laws that the programmes are meant to be following. It is not just a matter of reproducing the legislation, but of including the common law presumptions that underlie the legislation and the effects of the case law that has refined interpretation of the legislation. As Justice Melissa Perry of the Federal Court says:

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

⁷⁸ The following paragraphs draw upon Kerry Weste and Tamsin Clarke, “Human Rights Drowning In The Data Pool: Identity-Matching & Automated Decision-Making In Australia”, *Human Rights Defender*, Australian Human Rights Institute, (2018) Vol 27, Issue 3, p 25 ff.

⁷⁹ Simon Elvery, “Howe algorithms make important government decisions – and how that affects you”, 21 July 2017, ABC News online, <http://www.abc.net.au/news/2017-07-21/algorithms-can-make-decisions-on-behalf-of-federal-ministers/8704858>

⁸⁰ J Arvanitakis and A Francis (2018) ‘Data ethics is more than just what we do with data, it’s also about who’s doing it’, *The Conversation*, 22 June 2018, <<https://theconversation.com/data-ethics-is-more-than-just-what-we-do-with-data-its-also-about-whos-doing-it-98010>>

⁸¹ N Byrnes (2016) ‘Why We Should Expect Algorithms to Be Biased’, *MIT Technology Review*, 24 June 2016, <https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/>; D Cossins (2018) ‘Discriminating algorithms: 5 times AI showed prejudice’, *New Scientist Magazine*, 27 April 2018 available at <<https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/>>

⁸² L Edwards and M Veale (2017) ‘Slave to the Algorithm? Why a right to an explanation is probably not the remedy you are looking for’, *Duke Law and Technology Review*, Vol. 16, No. 1, p. 28, <<https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr>>

⁸³ See generally Cathy O’Neill, *Weapons of Math Destruction*, Penguin, 2017.

*the hierarchy between provisions determined. These are not necessarily simple questions and the potential for coding errors is real.*⁸⁴

- 9.6 The Robodebt debacle provides a clear example of reliance on a bad programme (and a bad system). Centrelink requires reporting of employment income, including casual employment and overtime payments, for fortnightly periods which include several days in the future from the reporting date. The system does not allow you to wait for your pay slip so you can give the accurate figures in retrospect. This practice therefore inevitably requires the Centrelink recipient to go back and correct the data when it turns out that they have been paid for more or fewer hours than they estimated would occur. As has been well publicized, access to a Centrelink officer is very difficult and thus attempting to report new data is also very difficult and time consuming.
- 9.7 Thus problems can easily arise with the efficacy of computer programmes. An additional problem is that their use is not transparent, and it can be difficult to identify how it is that, or whether or not, a computer programme has made a wrong decision. Administrative processes need to be transparent so that the decision-makers can be accountable.⁸⁵ To quote Justice Perry:

errors in computer programming and in the translation of complex laws into binary code can result in wrong decisions potentially on an enormous scale if undetected. Input errors may also lead to flawed decisions. Nor are all decisions by government of such a nature that they can appropriately or fairly be made by automated systems. The use of these systems by governments therefore raises questions as to the measures necessary to ensure their compatibility with the core administrative law values or principles that underpin a democratic society governed by the rule of law, in particular:

- *to ensure the legality of purported actions by public bodies;*
- *to guard against the potential erosion of procedural fairness; and*
- *to safeguard the transparency and accountability of government decisions by the provision of reasons and effective access to merits and judicial review.*⁸⁶

- 9.8 Even if the programmers had the expertise of judges and were required to create a ‘paper trail’ showing how all these elements are taken into account in their programme, such a paper trail might still not be comprehensible nor the programme perfect. Given that ‘[n]ot even the people who write algorithms really know how they work’ it is effectively impossible to render an algorithmic process completely transparent.⁸⁷
- 9.9 Justice Perry notes that programming errors may be replicated across many thousands of decisions undetected, and not until the outcomes reach catastrophic proportions will they be noticed (as with the Robodebt scenario). Where failures are less catastrophic, and thus less noticeable, the system's incorrect decisions may well remain hidden.⁸⁸

Applying this reasoning to technology-assisted decision-making, it is not enough for the executive to claim that it is using, or will use, technology in a way that promotes lawful decisions. There must be information available upon which the courts, integrity bodies and

⁸⁴ The Honourable Justice Melissa Perry, “iDecide: the Legal Implications of Automated Decision-making”, *Cambridge Centre for Public Law Conference 2014: Process and Substance in Public Law*, 15-17 September 2014, <<http://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20140915>>

⁸⁵ *ibid*

⁸⁶ *Ibid*, see also Dominique Hogan-Doran SC, “Accountability Mechanisms: Part III: Automated Decision-making”, 25 February 2017, *Law Council of Australia 2017 Immigration Law Conference*, at <https://static1.squarespace.com/static/568c9f234bf1182258eb9fbc/t/58b803cf37c58149faf5a5a7/1488454608349/Accountability+Mechanisms+Beyond+Merits+Review.pdf>

⁸⁷ A LaFrance, ‘Not even the people who write algorithms really know how they work’, *The Atlantic*, 18 September 2015, <<https://www.theatlantic.com/technology/archive/2015/09/not-even-the-people-who-write-algorithms-really-know-how-they-work/406099/>>

⁸⁸ Perry, *op cit*.

*the public can assess this question for themselves. Put another way: you may say that technology has assisted you to make a lawful decision, but how do I know that?*⁸⁹

Risk of loss and unauthorised access

9.10 The Federal Government itself does not have a good record of keeping personal sensitive information secure, contrary to the Australian Privacy Principles. In 2014 the Department of Immigration accidentally released the personal data relating to 10,000 asylum seekers.⁹⁰ And in 2016 the MBS/PBS dataset, containing health information about 10% of the entire Australian population, was released as ‘de-identified’ open data but was able to be decrypted so that doctors, and some of their patients, proved to be identifiable.⁹¹ The Minister for Law Enforcement and Cyber Security estimated that in 2017 there were 734 cyber incidents in private sector systems affecting the national interest.⁹²

9.11 According to Anna Johnston of Salinger Privacy:

A NSW auditor-general’s report found that two-thirds of NSW government agencies are failing to properly safeguard their data, by not monitoring the activities or accounts of those with privileged access to data, and one-third are not even limiting access to personal information to only staff with a ‘need to know’.

Leaving aside the question of why the NSW Privacy Commissioner is not resourced adequately to undertake these audits instead of needing the auditor-general to look into data protection, this report highlights a disturbing lack of compliance with the Data Security principle, which is neither new (NSW privacy legislation turns 20 this year) nor rocket science.

*Ignoring the privacy risks posed by staff misusing data is naïve; when I think of the more than 300 privacy cases against NSW public sector agencies over the past two decades, I cannot think of one that has involved a complaint arising from a disclosure to hackers, but countless have involved staff misusing the personal information to which they were given access.*⁹³

9.12 **When one comes to non-government APP entities, the picture is even bleaker.** Non-government entities will effectively be encouraged by the *Identity-Matching Services Bill 2018* to keep their own private databases of facial records – for checking against ‘the hub.’ APP entities are not subject to regular oversight by the Regulator, which relies on voluntary compliance by APP entities with the *Privacy Act* and associated *Australian Privacy Principles*. Problems only come to light through private complaints or self-reporting of breaches. And Equifax, one of the approved

⁸⁹ Katie Miller, “The Application of Administrative Principles to Technology-as-Decision-Making”, (2016) 86 *AIAL Forum* 20 at 25, <http://www7.austlii.edu.au/au/journals/AIAdminLawF/2016/26.pdf>

⁹⁰ Oliver Laughland, Paul Farrell and Asher Wolf, “Immigration Department data lapse reveals asylum seekers’ personal details”, *The Guardian Online*, 19 February 2014, at <https://www.theguardian.com/world/2014/feb/19/asylum-seekers-identities-revealed-in-immigration-department-data-lapse>.

⁹¹ Paris Cowan, “Health pulls Medicare dataset after breach of doctor details,” 29 September 2016, IT News online, at <https://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463> and Chris Culnane, Benjamin Rubinstein and Venessa Teague, “Understanding the Maths is crucial for Protecting Privacy”, 29 September 2016, Pursuit, University of Melbourne, at <https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy>

⁹² Amy Remeikis, “Australia warns businesses about sophisticated cyberattacks”, *The Guardian Online*, 10 October 2017 at <https://www.theguardian.com/australia-news/2017/oct/10/australia-warns-businesses-about-sophisticated-cyberattacks>

⁹³ “Too much cyber, not enough privacy 101” by Anna Johnston, *Salinger Privacy*, 5 February 2018 at <https://www.salingerprivacy.com.au/2018/02/05/not-enough-privacy-101/>

gateway service providers for the existing and similar Australian Document Verification System, recently breached security on the personal details of over 143 million US citizens.⁹⁴

- 9.13 The purported protection in section 7(4) of the *Identity-Matching Services Bill 2018* for individuals having their identities checked by local government or non-government bodies (which is that the body will have entered into an agreement to abide by rules along the lines of the *Australian Privacy Principles*) really provides very little protection in practice, particularly where the agreement relates to biometric data which of itself removes one of the key APP rights – to be anonymous or pseudonymous.

Integrity of Data

- 9.14 The related issue of the need to protect the integrity of data, including by retaining records of data provenance, data analysis, access or usage decisions, and establishing appropriate oversight and control mechanisms, is discussed by Data to Decisions Cooperative Research Centre at section 3.4 and following of their 2018 Report.⁹⁵

10 Examples

The following are some examples of recent legislation in the national security area which may be impractical and/or counterproductive and in relation to which the risk of error is real.

10.1 Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018

- 10.1.1 A leading IT expert, Dr Paul Henman of Queensland University, has submitted that the proposed Federal ‘hub’ holding drivers’ licence information from 8 different jurisdictions will be both a more expensive and a less efficient system than leaving the drivers’ licence information with the States and Territories and having those separate databases interrogated, if need be, from the Federal ‘hub.’⁹⁶ It indeed appears that there is less chance of hacking and more chance for State Governments to impose appropriate privacy restrictions on the use of their residents’ information under Dr Henman’s proposal – as opposed to what the Human Rights Law Centre calls a ‘**very high risk proposed regime**’ on the part of the Federal Government.⁹⁷

10.2 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

- 10.2.1 In the same year that Europe has introduced the General Data Protection Regulation in the interests of protecting the digital privacy of European citizens, Australia proposed legislation that would allow covert installation by government of programmes that are effectively malware into Australians’ computers and phones and would penalise people who refuse to give the government their passwords⁹⁸ with imprisonment for 10 years or 600 penalty units (being over \$120,000) or both -irrespective of whether or not any harm was involved. The contrast between concern for citizens’ rights in Europe – and lack thereof in Australia - could not be starker.
- 10.2.2 This Bill is impractical and could have serious cybersecurity and economic effects. This Bill breaches key privacy rights not only for Australians but for all customers of affected companies no matter where they may be in the world. The Bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider (telco/isp) to do an unlimited range of *acts or things*, which could mean anything from removing security measures to

⁹⁴ Elise Thomas, op cit.

⁹⁵ at p 172 ff and see 194 ff in relation to record-keeping.

⁹⁶ Submission 19, Inquiry Submissions page

⁹⁷ Submission 19, p 1, Inquiry Submissions page

⁹⁸ See definition of ‘access’ in section 317B.

deleting messages or collecting extra data. Providers will also be required to conceal any action taken covertly by law enforcement.

- 10.2.3 Further, the Attorney General may issue a “technical capability notice” *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency. Effectively it appears that companies may be required to provide confidential and sensitive information about how their systems work, and to assist the government in bypassing those companies’ security (particularly encryption) systems, if that is possible. The range of services providers covered would appear to include telecommunication companies, internet service providers, email providers, social media platforms and a range of other “over the top” services (any app or service that provides a product over the Internet and bypasses traditional distribution) as well as those who develop, supply or update software, and who manufacture, supply, install or maintain data processing devices.
- 10.2.4 If carried into effect, the measures would enormously increase the likelihood of new and uncontrollable computer threats and vulnerabilities worldwide through its proposed use against encryption. Weakening encryption weakens the entire Internet and increases risks for everyone on it.
- 10.2.5 As Access Now comments: *‘encryption protocols are the backbone of the digital economy, facilitating every single transaction online.’* The Bill appears to be aimed at reducing the security of encryption systems worldwide which could have disastrous and unforeseen effects internationally on both industry and governments. While we are not experts in this area (and so refer to the concerns expressed by many peak technological organisations), it is clear that the international implications of this Bill are of serious concern.
- 10.2.6 In addition to the serious human rights concerns that such broadly drafted and wide ranging measures give rise to, ALHR submits that the provisions are impractical. Major international corporations are extremely unlikely to meet the requirements that the Australian government might seek to impose upon them under the Bill, if it is enacted. It is not clear how the companies which are asked to assist the Australian government in such matters are expected to fund the work they are required to do nor how they are expected to cope with the consequential reputational damage, should their assistance in undermining their own systems become known.
- 10.2.7 **It would seem that, by disproportionately impinging upon everyone’s right to privacy, what the legislation is most likely to do is to drive criminal communications further underground, encouraging criminals to use devices that cannot be intercepted, while at the same time weakening or imperilling valid encryption methods used legitimately for world wide commerce and banking.**
- 10.2.8 Indeed, given that the recently expanded definition of ‘national security’ in section 90.4 of the Criminal Code now includes Australia’s economic relations with other countries, we query whether government agency actions pursuant to the Bill, should it become law, might actually involve breaches of Australia’s own national security. Government departments will not be immune from the very system weaknesses that the Bill seeks to create.

10.3 *Crimes Legislation Amendment (Police Powers at Airports) Bill 2018*

- 10.3.1 Professor Sarre argues that the proposed amendments in this legislation are likely to lead to loss of trust in police, thus in practice assisting rather than countering terrorism for two related reasons: because loss of trust in the police leads to people being less likely to obey the law and because it results in less information-sharing with police.⁹⁹ In his view, “(r)andom

⁹⁹ Sarre, op cit and see also Kurt Iveson, “To create safer cities for everyone, we need to avoid security that threatens”, 1 May 2018, *The Conversation*, < <https://theconversation.com/to-create-safer-cities-for-everyone-we-need-to-avoid-security-that-threatens-93421>>

stopping, questioning and demanding identification carries with it the risk of racial and social profiling, which brings with it public disquiet if not anger.... If that type of profiling occurs over and over, police quickly lose their 'legitimacy.' If [the community providing information to police] loses confidence in the police, then the well-spring of potentially significant information quickly dries up."¹⁰⁰

- 10.3.2 As Professor Sarre notes,¹⁰¹ it is difficult to imagine what the 'move on' directions (to not take flights and to stay out of airports) would be used for in practice. If police had real concerns about a person in an airport being likely to endanger anyone's safety, surely they would arrest them under existing powers?
- 10.3.3 There are already clear legislative powers to prevent suspicious persons from boarding planes and indeed everyone is familiar with the ultimate practical power of airlines to simply state that they have overbooked and that certain people will not be able to take a specific flight.
- 10.3.4 It is not clear what benefit to public safety there would be from police exercising the proposed 'move on' powers - while failing to arrest a person about whom they apparently harbour reasonable suspicions. On the other hand, the potential for severe inconvenience (and no doubt loss of prepaid air fares) to anyone who might be the subject of such police directions is clear. It is hard to envisage how the 'move on' powers could be used other than in a discriminatory manner, with the consequential problems identified by Professor Sarre.

10.4 *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*

Under this legislation, a 'foreign principal' does not include foreign businesses, but does include UN bodies. In responding to criticism of this drafting, the Committee appeared to suggest that if dealing with UN bodies were to be excluded from the relevant section, then spies would find a way to utilise such bodies in order to achieve their espionage ends.¹⁰² In our view, it is much more likely that spies would conduct espionage through the gap of foreign business rather than the so-called gap of UN bodies. The resulting legislation risks criminalising normal human-rights correspondence with UN bodies, as described above.

10.5 *Foreign Influence Transparency Scheme Act 2018*

While this legislation had the stated purpose of making foreign influence upon government transparent, in its final form it exempted all sitting parliamentarians. It is hard to see how this Act has resulted in anything but a 'name and shame' register for supposed foreign influencers. Crucial elements of the registration requirements relate to influencing a process, a concept which is not easy to understand. Originally the legislation referred to influencing a process but not its 'outcome'. That wording has now been removed, leaving it unclear whether or not the outcome of a process is regarded under the Act as part of the process.

11. Lack of Oversight

- 11.1 **While we acknowledge the importance of secrecy in relation to many issues of national security, at the same time it is essential that there be judicial, parliamentary and – to the maximum extent possible - public oversight of Australia's intelligence community in order to maintain the highest standards of behaviour, to support the rule of law in a democratic governmental system, and in order that those involved be accountable for their actions.**¹⁰³

¹⁰⁰ Sarre, op cit.

¹⁰¹ Sarre, op cit.

¹⁰² par 3.91 of the report in relation to the *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*

¹⁰³ Data to Decisions Cooperative Research Centre, op cit, Section 2.5.2, p 70 ff.

- 11.2 To achieve those often conflicting aims is inevitably a difficult balancing act but, we submit, one that is possible in accordance with the framework established by the principles of international human rights jurisprudence.
- 11.3 At present, the only oversight over intelligence community operations is at parliamentary executive level, being the oversight exercised by the relevant Minister over the particular intelligence organisation that he or she heads. Now that so many Ministries have been moved into the Home Affairs 'mega Ministry', the minimal checks and balances that applied through having different Ministers involved in intelligence community oversight would appear to be further diminished. We note also that government participants having policy roles who responded to the survey of intelligence operatives carried out by the Data to Decisions Cooperative Research Centre generally had difficulty articulating the exact accountability, transparency and oversight mechanisms relevant to them.
- 11.4 We support the removal of limitations on matters that can be considered by the Parliamentary Joint Committee on Intelligence and Security (PJCIS or 'the Committee') and the expansion of powers of the PJCIS to initiate its own reviews into operational matters¹⁰⁴.
- 11.5 We support the recommendation in *State of Digital Rights Report*, Digital Rights Watch, 2018 that the loopholes opened with the 2011 reform of the Freedom of Information (FOI) laws should be closed by returning ASD, ASIO, ASIS and other intelligence agencies to the ambit of the FOI Act, with the interpretation of national security as a ground for refusal of FOI requests being reviewed and narrowed.¹⁰⁵
- 11.6 **In relation to Senator Patrick's recent Bill:**
- we do not agree that court oversight should be excluded in relation to any exercise of Ministerial function (proposed section 29A(3)); and
 - we support the submission by the IGIS that mandatory functions should not be imposed on the office of the IGIS because of the fundamental concept that the IGIS must both act independently and be seen to be acting independently.
- 11.7 **We support the following measures either to increase oversight or because of existing lack of oversight:**
- a) introduction of a requirement for a judicial warrant to access users' metadata and the content thereof;
 - b) the right to full legal representation for persons the subject of an ASIO questioning warrant;
 - c) removal of ASIO's powers to detain individuals for questioning;
 - d) restrictions on the limits in the *National Security Information (Criminal and Civil Proceedings) Act 2004* upon full legal representation of the accused.
- 11.8 It is particularly unacceptable that under the *Australian Security Intelligence Organisation Act 1979 (Cth)*, questioning warrants may be used against non-suspects, including children, and that both the lawyer and the client may be monitored in what should be their confidential discussions by ASIO and are prohibited from disclosing the existence of the warrant or the fact of questioning.

12. Weakness of Australian Privacy Legislation¹⁰⁶

- 12.1 Privacy is a fundamental human right recognized in the UN *Declaration of Human Rights*¹⁰⁷, the *International Covenant on Civil and Political Rights* (ICCPR) and in many other international and

¹⁰⁴ *State of Digital Rights Report*, Digital Rights Watch, 2018, at <https://digitalrightswatch.org.au/2018/05/14/the-state-of-digital-rights/>.

¹⁰⁵ *Ibid*, p 8.

¹⁰⁶ See generally Tamsin Clarke, "Privacy Principles" in *State of Digital Rights Report*, op cit, p 14 ff.

¹⁰⁷ Article 12 states: "No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the

regional treaties. “Privacy,” comments one organisation, “underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.”¹⁰⁸

- 12.2 The *Privacy Act* provides for only limited civil redress, by way of complaints to the Australian Information Commissioner.¹⁰⁹ In 2014 the Australian Law Reform Commission made extensive recommendations in a document of over 300 pages for the introduction of a Commonwealth statutory civil cause of action for serious invasions of privacy, including digital privacy, following from three earlier enquiries which had supported this reform.¹¹⁰ We support the implementation of those recommendations.
- 12.3 We also support the other recommendations to strengthen Australian privacy law made in the *State of Digital Rights Report (2018)* by Digital Rights Watch.¹¹¹
- 12.4 The Commonwealth *Privacy Act* regulates collection and use of personal information through thirteen ‘Australian Privacy Principles’ but does not address surveillance, which is permitted for law enforcement agencies under various legislation.¹¹² Nor does it apply to Commonwealth intelligence agencies¹¹³ or State or Territory government agencies such as the NSW Police

law against such interferences or attacks.”

¹⁰⁸ Privacy International, *Privacy and Human Rights: an International Survey of Laws and Practice*, available at Global Internet Liberty Campaign < <http://gilc.org/privacy/survey/intro.html>>. See also *Methodology Report - Big Data Technology and National Security*, Data to Decisions Cooperative Research Centre, June 2018, p 21, and the literature cited at footnotes 91 to 93.

¹⁰⁹ Sections 36, 40, 52.

¹¹⁰ Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report 123, 2014), <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>, par 1.17.

¹¹¹ State of Digital Rights Report, Digital Rights Watch, 2018, at <https://digitalrightswatch.org.au/2018/05/14/the-state-of-digital-rights/>.

¹¹² The States have their own legislation. Relevant Commonwealth legislation includes: Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (‘TIA Act’) (relating to data retention obligations), the *Telecommunications Act 1997*, the *Intelligence Services Act 2001*, the *Surveillance Devices Act 2004* and the *Australian Federal Police Act 1979* (Cth), s 60A(2) of which allows federal police recording and retaining of personal information. The AFP is legally permitted to collect facial images where it is ‘reasonably necessary to fulfil its policing functions’ and share them when it is ‘reasonably necessary for law enforcement purposes’ Attorney-General’s Department (Cth), ‘Face Matching Services’ (Fact Sheet) 3 <<https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Fact-Sheet-National-Facial-Biometric-Matching-Capability.pdf>>.

¹¹³ Not covered are: the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate, the Defence Intelligence Organisation, the Australian Geospatial-Intelligence Organisation. Office of the Australian Information Commissioner, “Which law enforcement agencies are covered by the Privacy Act?” at <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement>.

Force.¹¹⁴ Some States have privacy legislation that regulates use of personal information by State and local government agencies,¹¹⁵ in some cases involving criminal sanctions.¹¹⁶

- 12.5 Even where the *Privacy Act* does cover law enforcement agencies, there are many exemptions. An entity covered by the Act can only use or disclose personal information for the purpose for which it was collected (the ‘primary purpose’) unless an exception applies, in which case the entity can also use or disclose that information for secondary purpose(s) (which need not be directly related). Exceptions include use or disclosure which is required or authorised by or under an Australian law or a court/tribunal order (Australian Privacy Principle 6.2(b)). Examples include where:
- a warrant, order or notice issued by a court requires the entity to provide information, or produce records or documents that are held by the entity;
 - the entity is subject to a statutory requirement to report certain matters to an agency or enforcement body; or
 - a law applying to the entity clearly and specifically authorises it to use or disclose the personal information.
- 12.6 Other exceptions which could be used by law enforcement agencies include:
- Lessening or preventing a serious threat to life, health or safety: (s 16A(1), Item 1).
 - Taking appropriate action in relation to suspected unlawful activity or serious misconduct: (s 16A(1), Item 2).
 - Reasonably necessary for establishing, exercising or defending a legal or equitable claim: (s 16A(1) Item 4).
- 12.7 A recent survey of personnel in Australian national intelligence agencies found that most respondents knew about the *Privacy Act* mainly from the point of view that their own organisation was exempt from the Act. They also tended to rely for their information about their privacy obligations upon internal organisation manuals and protocols rather than the legislation itself.¹¹⁷ Nonetheless, the survey appears to indicate a culture of privacy compliance surrounding data retention and use within the Australian intelligence community¹¹⁸, and a concern for breaches at other levels, for example by State police.¹¹⁹
- 12.8 At the same time, it should be noted that there do not appear to be any laws regulating access to, or use of, ‘open source’ information by federal or state law enforcement or national intelligence agencies, nor restrictions upon acquiring information from private sector data brokers.¹²⁰

¹¹⁴ Office of the Australian Information Commissioner, “Which law enforcement agencies are covered by the Privacy Act?” at <https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement>. It should be noted that the Australian Government Agencies Privacy Code (available at <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017>) was registered on 27 October 2017 and comes into effect on 1 July 2018. It is a relatively short document which sets out specific requirements for government agencies to which the Privacy Act applies to assist them in adopting a best practice approach to privacy governance.

¹¹⁵ *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Premier and Cabinet Circular No 12* (SA); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic); *Information Privacy Act 2014* (ACT); *Information Act* (NT).

¹¹⁶ Under s 62 of the *Privacy and Personal Information Protection Act 1998* (NSW) the unauthorised or corrupt use or disclosure by a public official of personal information obtained through their official functions is an offence punishable by up to 100 penalty units or imprisonment for up to two years.

¹¹⁷ Data to Decisions Cooperative Research Centre, op cit, p 66 ff.

¹¹⁸ Data to Decisions Cooperative Research Centre, op cit, section 2.5.3, p 73 ff.

¹¹⁹ Data to Decisions Cooperative Research Centre, op cit, p 54.

¹²⁰ Data to Decisions Cooperative Research Centre, op cit, p 135.

12.9 Today, digital rights in relation to free and private communication are essential in order that *all* human rights can be protected and realised.¹²¹ Indeed many countries have expressed internet access to be a national right. However, digital rights are increasingly restricted by governments, including Australia, in the name of national security.

12.10 **Digital rights** are an aspect of human rights and include the rights:

- (a) to communicate freely through electronic devices and communications networks, including the internet, without harassment (relevant to freedom of expression¹²² and association¹²³ cultural participation¹²⁴ and self-determination¹²⁵ and freedom from discrimination¹²⁶);
- (b) to privacy¹²⁷ of electronic communication, including the rights to be anonymous, to have one's movements¹²⁸ and both the content of one's communications and one's 'digital footprint' kept private, free from collection or surveillance;
- (c) to have control over one's personal data and not have it misused or stolen (rights to privacy, to be free from discrimination¹²⁹ and to preserve one's reputation¹³⁰); and
- (d) to have legal redress where one's rights are infringed.¹³¹

12.11 More broadly, the idea of digital rights also encompasses privacy and security issues around the collection and use of information about a person held in digital form, whether that is biometric data, movement data from phones, travel cards, airlines, border crossings or numberplate recognition, to e-health, commercial and financial information.

12.12 Breaches of digital rights involving "intrusion upon seclusion," such as by physically intruding into a person's private space or by watching, listening to or recording the plaintiff's private activities or private affairs; or "misuse of private information," such as by collecting or disclosing private information about a person, are regarded by the Australian Law Reform Commission as a 'serious invasion of privacy.'¹³²

¹²¹ Association for Progressive Communications, <https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter>.

¹²² Article 19 of the *Universal Declaration of Human Rights 1948* (UDHR), Article 19 of the *International Covenant on Civil and Political Rights 1966* (ICCPR), Theme 2 of the Association for Progressive Communications (APC) *Internet Rights Charter 2001* at <https://www.apc.org/en/node/5677> (APC Charter).

¹²³ Article 20 UDHR, Article 20 ICCPR.

¹²⁴ Article 27 UDHR, and Articles 1.1, 3 and 15(a) of the *International Covenant on Economic, Social and Cultural Rights 1966* (ICESC), Themes 3 and 4 of the APC Charter

¹²⁵ Article 1.1, ICCPR and Article 1.1 ICESC.

¹²⁶ Articles 2 and 7, UNHR, Articles 2 and 26, ICCPR.

¹²⁷ Article 12 of the UDHR, Article 17 of the ICCPR, Theme 5 of APC Charter, and see too the *International Principles on the Application of Human Rights to Communications Surveillance 2014* (also known as "Necessary and Proportionate") (May 2014) at <http://necessaryandproportionate.org/principles>

¹²⁸ Article 13, UNHR.

¹²⁹ As the US Federal Trade Commission noted, "use of big data analytics to make predictions may exclude certain populations from the benefits society and markets have to offer" - US Federal Trade Commission, *Big Data: A tool for inclusion or exclusion?* January 2016, p 9, accessed at: <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>, pages 8 and 9.

¹³⁰ Article 12, UNHR, Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report 123, 2014), <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>, Recommendations (unnumbered page towards the front of the report)

¹³¹ Articles 2(3) and 17 of the ICCPR.

¹³² Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report 123, 2014), <https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>, Recommendations (unnumbered page towards the front of the report)

12.13 Because Australia inherited the English common law, not a civil law, system and did not adopt a bill of rights in its Constitution, Australia does not have a human rights framework to protect digital rights. The Commonwealth *Privacy Act*¹³³ is very limited. There is no tort of privacy under Australian law and the common law offers a very inadequate protection for human rights such as privacy. In addition the common law can be overridden by contrary legislation. The result is a 'significant governance gap'.¹³⁴

12.14 **Much legislation that relates to national security references the Australian Privacy Principles, while effectively overriding those principles or ignoring their general weakness. Examples are:**

The Identity-Matching Services Bill 2018

- It is a fundamental aspect of the *Australian Privacy Principles* that individuals should know the reason for collection of their personal information and that the information should be used only for that particular purpose or purposes. **This fundamental concept is not honoured** by the *Identity-Matching Services Bill*, which indeed specifically provides that data obtained for one purpose can be used for other purposes, with section 3 providing that: 'The Department may use or disclose **for any of those purposes** information so collected **(regardless of the purpose for which it was collected)**' (emphasis added). The information may also be shared with other countries, amounting to a substantial breach of personal privacy.
- The Facial Verification Service described in section 10 of the Federal Bill can be accessed by local councils and non-government entities. This could result in the sale of sensitive personal information for commercial purposes. While some purported protections are included in sections 7(3) (consent of individual) and 7(4) (application of Australian Privacy Principles) these protections would appear to be of little use in practice as consent is effectively forced, not free.
- Thus in order to be able to drive in NSW one must 'consent' to have one's photograph taken, and reproduced on one's driver's licence. However Australians are not being asked if they wish their State driver's licence information to be shared with the Commonwealth pursuant to this legislation, and it is likely that consent in other contexts, like identity verification by banks before one can open a bank account, will effectively be a forced consent. We have no opportunity to 'opt out' of this system which is being imposed with no public discussion.
- The cavalier approach taken to biometric privacy under this legislation needs to be contrasted with the strong privacy protections in European jurisdictions and even some US States (compare with the *Illinois Biometrics Information Privacy Act*.¹³⁵

Amendments to the Telecommunications (Interception and Access) Act 1979

- While Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* requires all service providers that collect and retain telecommunications data under the data retention scheme to comply with the Privacy Act in relation to that data, there are no requirements in the Privacy Act to keep the data in Australia, and it is reasonable to fear that the data could be stolen or hacked.

¹³³ The Act applies to most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses— see <https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10>.

¹³⁴ Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSW Law JI 6; (2017) 40 (1) University of New South Wales Law Journal 121, at 122.

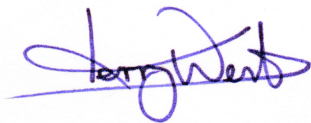
¹³⁵ See footnote 145, Data to Decisions Cooperative Research Centre, op cit, p 137. Under this Act, Facebook was sued for its failure to obtain written consent to the harvesting of personal images.

13 Conclusion

- 13.1 Any legislation which impinges upon human rights must be narrowly framed, **proportionate** to the relevant harm, and provide an appropriate contextual response which minimises the overall impact upon all human rights, democracy and the rule of law.
- 13.2 Given that Australians are alone amongst Western democracies in not having a federal Human Rights Act to expressly legally protect their rights, all oversight of the extensive intelligence powers that have been expanded over recent years is to be encouraged and we **commend the use of a human rights framework to the Review, as described above in section 3**, as a useful and essential process which will assist the aims of the Review.

If you would like to discuss any aspect of this submission, please email me at: president@alhr.org.au

Yours faithfully



Kerry Weste
President
Australian Lawyers for Human Rights

Any information provided in this submission is not intended to constitute legal advice, to be a comprehensive review of all developments in the law and practice, or to cover all aspects of the matters referred to. Readers should obtain their own legal advice before applying any information provided in this document to specific issues or situations.

Appendix: Recent legislation which has impinged upon Australians' human rights in the name of national security (or proposes to do so)

Australian Citizenship Amendment (Allegiance to Australia) Act 2015

Australian Passports Amendment (Identity-matching Services) Bill 2018 (Cth)

Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014

Counter-Terrorism Legislation Amendment Act (No.1) 2016

Crimes Legislation Amendment (Powers, Offences, and Other Measures) Bill 2015, 2017, 2018

Crimes Legislation Amendment (Police Powers at Airports) Bill 2018

Criminal Code Amendment (Impersonating a Commonwealth Body) Act 2018

Foreign Influence Transparency Scheme Act 2018

Home Affairs and Integrity Agencies Legislation Amendment Act 2018

Identity Matching Services Bill 2018 (Cth)

National Security Legislation Amendment Act (No. 1) 2014

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018

Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth)