Human Rights Law Centre

A dangerous lack of accountability and transparency in Australia's national intelligence organisations

Submission to the Comprehensive Review – Legal Framework of the National Intelligence Community

12 December 2018

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Prepared by

Alice Drury (Lawyer) and Hugh de Kretser (Executive Director) **Human Rights Law Centre** with assistance from Lizzie O'Shea, **Digital Rights Watch**

Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 44
F: + 61 3 8636 4455
E: alice.drury@hrlc.org.au
W: www.hrlc.org.au

Human Rights Law Centre

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

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

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

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, lobby and advocate for a digital environment where individuals have the power to maintain their human rights.

W: www.digitalrightswatch.org.au

Contents

1. Introduction

The Human Rights Law Centre (**HRLC**) welcomes the opportunity to make a submission to the comprehensive review of the legal framework governing the national intelligence community (**Review**). We welcome the Review's commitment to ensuring that the legislative framework contains consistent protections for Australians.

This submission builds on the HRLC's substantial work responding to encroaching national security legislation addressing:

(a) the role of the Independent National Security Legislation Monitor (**INSLM**) in 2009,[1] 2014[2] and 2015;[3]

(b) sweeping new counter-terrorism powers proposed in 2010[4] and 2014;[5]

(c) metadata storage and access laws;[6] and

(d) in 2018, laws broadening espionage and secrecy offences,[7] and expanding the use of facial images and biometric data.[8]

The HRLC has consistently raised concerns that the rapidly growing body of national security legislation poses an unacceptable threat to Australians' human rights. The current legislative framework also suffers from a lack of government accountability and transparency measures, which undermines Australia's democracy.

There is much that HRLC could say on specific provisions within the enormous body of national security legislation, but consistent with the broad terms of reference of this Review, this submission focuses on improving the existing legal infrastructure that establishes accountability and transparency of our national intelligence agencies.

---

[1] Human Rights Law Centre and Public Interest Law Clearing House, Joint Submission to the Finance and Public Administration Legislation Committee, *Inquiry into the Independent National Security Legislation Monitor Bill 2009*, July 2009.

[2] Human Rights Law Centre, Submission to Senate Legal and Constitutional Affairs Committee, *Committee Review of the Act to Repeal the Independent National Security Legislation Monitor Act 2010*, 5 May 2014.

[3] Human Rights Law Centre, Submission to Senate Legal and Constitutional Affairs Committee, *Inquiry on the Independent National Security Legislation Monitor (Improved Oversight and Resourcing) Bill 2014*, 29 January 2015.

[4] Amnesty International and Human Rights Law Centre, Submission to Senate Standing Committee on Legal and Constitutional Affairs, *Inquiry on the Independent National Security Legislation Monitor Bill 2010*, 30 April 2010.

[5] Human Rights Law Centre, Submission to Australian Law Reform Commission, *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws Issues Paper*, 27 February 2014.

[6] Human Rights Law Centre, Submission to the Attorney-General, *Retained Data in Civil Proceedings Consultation*, 25 January 2017.

[7] Human Rights Law Centre, Submission to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the National Security Legislation Amendment (Espionage and Interference) Bill 2017*, 22 January 2018.

[8] Human Rights Law Centre, Submission to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into the Identity-Matching Services Bill 2018 and the Australian Passports Amendment (Identity-Matching Services) Bill 2018*, 29 May 2018.

2. Background: broader powers without proper accountability

This Review is important. To paraphrase the 2017 Independent Intelligence Review (**2017 Review**), the national security landscape in Australia is facing new and increasingly complex challenges, including new forms of rivalry among states, extremism with global reach and accelerating technological change.[9] This has been the justification for the enormous number of ad hoc bills (72 at the time of this submission) that have passed through Parliament since 11 September 2001, frequently without enough time for proper public consultation. Simultaneously, the resourcing of our intelligence agencies has tripled or more over that period.[10]

More to the point however, the sheer impact of the laws that have passed Federal Parliament since 2001 is staggering. The abrogation of human rights through extensive stop and search powers, questioning powers, control orders and preventative detention orders is unprecedented.[11] Harsh penalties – up to life imprisonment – apply to journalists, advocates and whistleblowers who disclose illegal and wrongful conduct by the Government where it causes "harm" to national security.

But perhaps the most significant development is that millions of Australians and others are now subjected to mass surveillance without judicial oversight. International digital rights advocacy group Access Now have described it as "one of the most extensive surveillance legal schemes in the world", and listed Australia alongside Egypt, Kazakhstan, Russia and Turkey as a "country under surveillance".[12] The decryption and proposed facial recognition laws will make this situation much worse.

Despite all of this extraordinary reform, there have been few attempts to improve public accountability and transparency over the agencies in 40 years.

There are a number of reasons contributing to this asymmetrical law reform that has undermined human rights protections to a degree not experienced in similar countries.

One key factor is a political culture where both major parties have been unwilling to publicly oppose proposals for ever-expanding investigative and coercive powers sought by national intelligence agencies. This bipartisan deadlock has in turn been exacerbated by intensive and unjustified secrecy and institutional barriers to crossbench and public scrutiny of the powers and operations of intelligence agencies. The absence of a constitutional or legislative charter of human rights in Australia has contributed further. Australia is the only Western democracy without a charter or bill of rights meaning our national security reforms have not been subjected to the same human rights scrutiny and

---

[9] M L'Estrange and S Merchant, *2017 Independent Intelligence Review Report*, June 2017, 5.

[10] For instance, as at 30 June 1999, ASIO had 565, that number is now 1815. ASIO's budget also expanded commensurately from $65.7 million in 1999-2000 to $518 million (estimated actual) in 2016-17: see J Faulkner, "Surveillance, Intelligence and Accountability: an Australian Story", 24 October 2014.

[11] As illustrations of how serious these measures are, the HRLC draws the Review's attention to the wrongful imprisonment and solitary confinement of Kamer Nizamdeen and Mohamed Haneef.

[12] Access Now, 'Human Rights in the Digital Age: An International Perspective on Australia' 4 <https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf>.

accountability that has occurred in nations like the United Kingdom, New Zealand, Canada and the United States.

This analysis forms the basis for the recommendations in this submission, which seek to:

(a) centre parliamentary oversight, rather than executive oversight, over intelligence agencies to improve public accountability;

(b) improve the quality and diversity of public debate on national security laws by enabling crossbench participation in the parliamentary review process;

(c) strengthen the Independent National Security Legislation Monitor (**INSLM**) so that the major parties must respond to concerns raised regarding proportionality and civil liberties;

(d) restore important pillars of public scrutiny of intelligence agencies by broadening judicial review, freedom of information (**FOI**) access and whistleblower protections; and

(e) confine the circumstances in which the extensive powers granted to intelligence and enforcement agencies can be used to protect economic interests.

The HRLC strongly encourages the Review to incorporate a robust accountability framework addressing the following recommendations in any proposal for holistic reform to national security legislation.

Recommendation 1:

The Inspector-General of Intelligence and Security should provide annual reports, reports on the conclusion of inquiries and reports following public interest disclosures to the Parliamentary Joint Committee on Intelligence and Security rather than the Attorney-General or the relevant Minister. It should then be for the PJCIS to determine what information should be withheld, according to suitably strict criteria and in consultation with the IGIS, prior to tabling the report in Parliament.

Recommendation 2:

The Independent National Security Legislation Monitor's powers should be broadened so that it may review all legislation relating to intelligence and national security, including prospective legislation, of its own motion. The Government should be required to respond to the Independent National Security Legislation Monitor's recommendations. Finally, consideration must be given to strengthening mechanisms to ensure sufficient time for proper review and consultation on proposed national security and intelligence laws.

Recommendation 3:

The Parliamentary Joint Committee on Intelligence and Security's scope of review should be broadened to operational matters, either generally or to allow it to receive, review and assess reports from the Inspector-General of Intelligence and Security.

Recommendation 4:

The membership of the Parliamentary Joint Committee on Intelligence and Security should be changed so that it includes at least two members from the crossbench.

Recommendation 5:

The Review should conduct a comprehensive assessment into where judicial oversight is lacking, and recommend that it be strengthened accordingly.

Recommendation 6:

There should be an avenue for external disclosures of intelligence information that do not pose a risk to national security and that serve the public interest. Further, that harsh penalties for whistleblowers and journalists be repealed.

Recommendation 7:

The Freedom of Information Act should apply to all intelligence agencies.

Recommendation 8:

The functions of the Australian Secret Intelligence Service should be clarified and narrowed as they relate to national economic well-being. The functions of the Australian Security Intelligence Organisation should be reviewed so as to exclude functions related to economic well-being and should explicitly be limited to protect Australians' freedoms of expression, association and assembly.

3. National security in the absence of a human rights charter

Australia is the only Western democracy that does not have a national charter or bill of rights. George Williams AO has observed that as a result, "we have many laws on our books with no comparison in the United Kingdom, the United States and other places that have a high threat level but also have a bill of rights that holds back parliaments from crossing the line".[13] These laws include extensive detention orders, forced questioning and speech offences.[14]

A national charter of human rights would provide an effective legal framework against which to assess the adequacy and necessity of national security powers. A charter would recognise the legal obligation of governments to protect our safety but would require governments to achieve that aim in a way that is reasonable and proportionate and that does not unnecessarily trample on fundamental rights like freedom from arbitrary detention, freedom of speech, association, assembly and privacy.

We would be very happy to provide a further, detailed submission on how a charter would assist to provide clear, consistent protections for Australians in this context, drawing on the experience of comparable countries such as the United Kingdom.

Further, in the absence of a charter of rights in Australia, appropriate parliamentary, judicial and public scrutiny is even more important, underscoring the importance of this Review.

4. Transparency and accountability

4.1 Background

The current framework for national security legislation was established in accordance with the principles set down by Justice Robert Hope in the Royal Commissions of 1974-1977 and 1984 (**Hope Reviews**). Those principles relevantly included executive and parliamentary oversight over the agencies through the establishment of the Inspector-General of Intelligence and Security (**IGIS**) and the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**).

As far back as 14 years ago, the Hon Philip Flood AO acknowledged in the Report of the Inquiry into Australian Intelligence Agencies (**Flood Review**) that the Hope Reviews were conducted in a context vastly different to the contemporary challenges we face today. The Flood Review noted changes such as the shift in focus from state-based intelligence to non-state terrorism, a greater public interest in intelligence matter and a huge increase in resources dedicated to the agencies. The review concluded

[13] G Williams, "A Charter of Rights for Australia "More Urgent than Ever", *UNSW Law Blog*, (2 August 2017) available at http://www.law.unsw.edu.au/news/2017/08/charter-rights-australia-more-urgent-ever.

[14] P Gregoire, "The Need for a Bill of Rights: an interview with UNSW Professor George Williams", (4 November 2017) available at https://www.sydneycriminallawyers.com.au/blog/the-need-for-a-bill-of-rights-an-interview-with-unsw-professor-george-williams/.

that this made the need for a "robust, effective and occasionally intrusive system of accountability" even greater vis-à-vis other government branches.[15]

The impact of laws introduced since the Flood Report has escalated dramatically again. Never before have Australian governments held or had access to such a staggering amount of data and metadata about each citizen. This unparalleled development affects every person in Australia and many overseas. Accountability and transparency measures established 40 years ago are not up to this task.

Further, the focus of accountability over national intelligence agencies has been on executive oversight. Parliamentary and judicial oversight has been limited, undermining the notion that the three arms of government keep one another in check.[16]

One of the justifications for executive oversight and ministerial responsibility is that, through the media and come election time, ministers will be held accountable to the Australian people for the activities of intelligence agencies within their portfolios. However the intensive secrecy around national intelligence operations and the trend towards the aggressive investigation and prosecution of whistleblowers means that these accountability measures are diminished.

Eminent academics in this field, George Williams AO and Keiran Hardy, have documented the increasingly close relationship between Ministers and intelligence agencies.[17] Expanding the powers of the intelligence agencies is perceived as granting a clear political benefit to politicians. Thus, it is not in the interests of the Attorney-General or other Ministers in Government to reveal important details of misconduct and illegality of intelligence agencies, and there is no way of knowing what the basis for omitting such details, or entire IGIS reports from public view, is. This does little to reassure that public accountability is valued by the responsible Ministers.

4.2 Executive oversight – the IGIS

(a) *Operation of the IGIS*

The most significant body that provides oversight over the legality and propriety of the operations of intelligence agencies is the independent statutory office of the IGIS, established under the *Inspector-General of Intelligence and Security Act 1986* (Cth) (**IGIS Act**). The IGIS assesses whether the six intelligence agencies have complied with applicable laws and ministerial guidelines, and whether the agencies have acted with propriety and consistently with human rights.

The IGIS conducts regular inspections of each agency and can make inquiries into complaints, which may come from the Prime Minister, members of the public, and people within the agencies themselves. The IGIS has similar powers to a royal commission, such as requiring the production of

[15] P Flood, *Report of the Inquiry into Australian Intelligence Agencies,* 20 July 2004, 51. Ultimately, the recommended amendments to accountability measures were minimal and, in the opinion of the HRLC, inadequate.

[16] K Hardy, G Williams, "Executive Oversight of Intelligence Agencies in Australia" in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, ed. Z Goldman and S Rascoff, (Oxford University Press, New York, 2016), 318.

[17] K Hardy, G Williams, "Executive Oversight of Intelligence Agencies in Australia" in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, ed. Z Goldman and S Rascoff, (Oxford University Press, New York, 2016), 334.

documents, visiting intelligence agency premises and inspecting documents, examining witnesses and requiring that questions be answered (criminal sanctions can be applied if misleading answers are provided). The IGIS is the sole recipient of public interest disclosures of intelligence information outside of the agency itself, under the *Public Interest Disclosure Act 2013* (Cth) (**PIDA**).

The IGIS is a powerful office which is currently held by a respected former Federal Court judge, the Honourable Margaret Stone.

(b) ***Limitations on transparency and accountability***

However, the IGIS office is weakened by the fact that it reports to Ministers, rather than to Parliament.

The HRLC notes that the annual report must be provided to the Leader of the Opposition as well as the Attorney-General under section 35 of the IGIS Act and an edited form of the report must be tabled before both Houses of Parliament and made public via its website. Information that is withheld from Parliament and the public rests within the sole discretion of the responsible Minister or, in the case of the annual report, the Attorney-General.[18]

Public interest disclosures in intelligence matters provide an example of this lack of transparency. In the four reporting periods since the PIDA has been in force, progressively less detail regarding public interest disclosures has been provided in annual reports. In the reporting period 2014/2015, the subject matter and reason for resolution of each disclosure was provided; in 2017/2018, no meaningful detail was provided for six out of the seven disclosures in that period.

This lack of transparency is compounded as, unlike normal public interest disclosures, there is no avenue open to a person to make public anything falling within the broad definition of "intelligence information" (see section 41 of the PIDA). If either the IGIS or the Minister responsible decide that an investigation is not warranted, or the results of an investigation should not be revealed publicly, there is no avenue for challenge and the public will never be any the wiser. This is even the case where disclosure of the "intelligence information" would be in the public interest, and would not in any way prejudice Australia's national security (see further recommendations regarding whistleblower protections in part 3.6 below).

(c) ***Recommendations***

The HRLC recommends that a new legal framework governing national security agencies establish a direct reporting relationship between the IGIS and Parliament via the PJCIS. It is common practice for an integrity agency, such as the Australian Commission for Law Enforcement Integrity and the Australian National Audit Office at Commonwealth level, or integrity commissioners at state level, to report to a relevant parliamentary committee. This reporting structure further aligns with the

[18] Under section 35(5) of the IGIS Act, the Attorney-General "may make such deletions from a report … as the Attorney-General considers necessary in order to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals".

recommendations of the 2017 Independent Intelligence Review,[19] and is more consistent with the UK system, in which the role of the IGIS is performed by a cross-party parliamentary committee directly.

It follows that on receiving the IGIS' reports, the PJCIS, in consultation with the IGIS and any relevant agency, would determine what information should be made public and what should be withheld on the basis that withholding was necessary to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals.

Further, the HRLC supports the IGIS' submission to the Review that it have access to the requisite expertise in relation to current technologies to effectively hold agencies to account. This expertise must be independent so that the IGIS is not wholly or substantially dependent on the technical assistance of the agencies subject to oversight.[20]

Recommendation 1:

The Inspector-General of Intelligence and Security should provide annual reports, reports on the conclusion of inquiries and reports following public interest disclosures to the Parliamentary Joint Committee on Intelligence and Security rather than the Attorney-General or the relevant Minister. It should then be for the PJCIS to determine what information should be withheld, according to suitably strict criteria and in consultation with the IGIS, prior to tabling the report in Parliament.

4.3 Legislation review – the INSLM

The utility of holding intelligence agencies accountable for breaches of the law is compromised when the legal thresholds that the intelligence agencies need to meet are too low. It is vital that the powers our Parliament confers on intelligence agencies are restricted to only those strictly necessary to defend against threats to Australia's security, properly defined.[21]

However, this is not the case in much of the national security legislation. To take just one example, the legislative threshold for Australian Security Intelligence Organisation (**ASIO**) officers to access communications is so broadly drafted under sections 175 and 176 of the *Telecommunications*

[19] M L'Estrange and S Merchant, *2017 Independent Intelligence Review Report*, June 2017, recommendation 23, [7.45]. The report recommended an expansion of the PJCIS's functions to request the IGIS to inquire into operational matters and provide reports to the PJCIS.

[20] M Stone, *Legal Framework of the National Intelligence Community: Initial submission on oversight-related legislation*, 14 August 2018, 13.

[21] To echo the IGIS in her submission to this Review, "as the exercise of agency powers will in the vast majority of cases not be apparent to the subject, and as they are by their nature often highly intrusive, these powers should only be considered for use when other, less intrusive, means of obtaining information are likely to be ineffective or are not reasonably available": M Stone, *Legal Framework of the National Intelligence Community: Submission to the Comprehensive Review*, 7 September 2018, 9.

(Interception and Access) Act 1979 (Cth),[22] that even the most intrusive access would likely be found by IGIS to be proper and lawful conduct.

Thus the INSLM provides a much-needed check on the extraordinary powers granted to intelligence and security agencies. Under the *Independent National Security Legislation Monitor Act 2010* (Cth) (**INSLM Act**), the INSLM assesses whether counter-terrorism and national security laws contain appropriate safeguards for protecting the rights of individuals and remain proportionate and necessary to any threat to national security.

However, there are significant restrictions on the INSLM that undermine the office's effectiveness, and a worrying trend of governments disregarding the INSLM's recommendations.

A number of issues need to be addressed in this context. First, the INSLM should be empowered to review proposed, as well as existing, legislation. Second, it should be empowered to review all counter terrorism and national security legislation of its own motion. Currently, "own motion review" by the INSLM is restricted to reviews of only select provisions of the legislation specified in section 4 of the INSLM Act. This means many intrusive, indiscriminate national security laws are not subject to review by the INSLM, unless referred by the Prime Minister or Attorney-General. For example, metadata retention laws, facial recognition and biometric data sharing and decryption laws have not been reviewed by the INSLM.

Further, the HRLC is deeply concerned that recommendations of the INSLM have been frequently ignored and, on occasion, strategically obfuscated by the Government.[23] To address this, the INSLM's scope of own motion review should not only be broadened, but the Government should be required to respond to the INSLM's recommendations. The HRLC also notes the 2017 Review's recommendation that the INSLM have a direct reporting relationship with the PJCIS, which could further enhance the impact of the INSLM's advisory function.[24]

The insufficiency of review of national security and intelligence legislation has been compounded by the tendency of Coalition Governments to expedite the passage of controversial legislation despite – or perhaps because of – significant opposition from civil society and experts. Recent and current examples include:

(a) metadata retention laws *(Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth))*;

[22] The officer need only be satisfied that the disclosure would be "in connection with the performance by the Organisation of its functions or the exercise of its powers". As submitted by the IGIS, "[a]lthough the intrusiveness of metadata collection has changed the legislative threshold has not": M Stone, *Legal Framework of the National Intelligence Community: Submission to the Comprehensive Review*, 7 September 2018, 6.

[23] K Hardy, G Williams, "Executive Oversight of Intelligence Agencies in Australia" in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, ed. Z Goldman and S Rascoff, (Oxford University Press, New York, 2016), 335. See also the criticism of former INSLM Bret Walker SC in *Annual Report 2013/2014*, 28 March 2014, 2.

[24] M L'Estrange and S Merchant, *2017 Independent Intelligence Review Report*, June 2017, [7.34].

(b) legislation imposing long prison sentences on journalists who report on Government illegality or misconduct during special intelligence operations (section 35P of the *National Security Legislation Amendment Bill (No.1) 2014 (Cth)*);

(c) life sentences for journalists and advocates who "deal" with information that might harm Australia's international interests (*National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth)* (**EFI Act**)); and

(d) decryption laws with reported major implications for the security of personal information (*Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth)*).

Consideration must be given to strengthening mechanisms to ensure proper review and consultation on proposed new national security and intelligence laws. This could include mechanisms to ensure sufficient time for the PJCIS and INSLM to review proposed laws, and to require the Government to respond to the INSLM's recommendations before a bill can pass. These mechanisms would need to allow flexibility for bills to be expedited where there are genuine exceptional circumstances.

We note that a bill that would have seen many of these reforms – the *Independent National Security Legislation Monitor (Improved Oversight and Resourcing) Bill 2014* (Cth) – was unfortunately allowed to lapse in 2016. The HRLC recommends that the Review revisit this bill in conjunction with the concerns raised here.

Recommendation 2:

The Independent National Security Legislation Monitor's powers should be broadened so that it may review all legislation relating to intelligence and national security, including prospective legislation, of its own motion. The Government should be required to respond to the Independent National Security Legislation Monitor's recommendations. Finally, consideration must be given to strengthening mechanisms to ensure sufficient time for proper review and consultation on proposed national security and intelligence laws.

4.4 Parliamentary oversight – the PJCIS

The PJCIS is currently able to review proposed legislation and the expenditure and administration of the six intelligence agencies. It is not empowered to review the operations of the agencies.

The oversight function of the PJCIS is significantly behind its equivalent in the UK. The Intelligence and Security Committee of UK Parliament (**ISC**) is an independent parliamentary committee established under the *Intelligence Services Act 1994*. The ISC is tasked with overseeing the expenditure, administration, policy and operations of UK intelligence agencies. The ISC is able to consider operational matters, albeit in limited circumstances,[25] and security agencies are required to disclose requested information to the committee. Further, and consistent with Recommendation 1

[25] Parliamentary Library, "Oversight of intelligence agencies: a comparison of the "Five Eyes" nations", *Research Paper*, 15 December 2017, 40.

above, redactions to reports are carefully considered by the Committee itself, and made only if the agencies clearly demonstrate how the publication of the material would be damaging to national security.[26]

In a 2014 report on Australian oversight of intelligence agencies, Senator John Faulkner observed that the UK amendments that allowed the ISC to oversee the operational activities of the agencies and secondly the power to require information rather than request it offered "much food for thought".[27]

The potential for expanding the scope of PJCIS' review to operational matters is currently a live issue before Parliament with Senator Rex Patrick's *Intelligence Services Amendment (Enhanced Parliamentary Oversight of Intelligence Agencies) Bill 2018* (Cth). The Senate Finance and Public Administration Legislation Committee recommended that the Bill not pass the Senate, in part pending the outcome of this Review. The HRLC notes that there were issues with this Bill, including the exclusion of judicial review and the potential to undermine the independence of the IGIS. However the core purpose of the Bill, in improving accountability and transparency, is sound.

The HRLC recommends that the Review consider expanding the powers of the PJCIS to review operational matters. This can be done broadly, as provided for in Senator Patrick's Bill, or by allowing the PJCIS to receive, review and assess reports made to it by the IGIS (see Recommendation 1).

Recommendation 3:

The Parliamentary Joint Committee on Intelligence and Security's scope of review should be broadened to operational matters, either generally or to allow it to receive, review and assess reports from the Inspector-General of Intelligence and Security.

The HRLC also supports reforms that would diversify the membership of the PJCIS. As outlined above, the major parties' commitment to bipartisanship on national security issues means that often only the most egregious aspects of proposed legislation is amended. This accounts for the vastly expanded power and resources of the intelligence agencies with few corresponding improvements in oversight and accountability.

The PJCIS and its predecessors have been comprised of six Government and five Opposition members and, with the exception of independent MP Andrew Wilkie from 2010-2013, no members from the crossbench. This means that the crossbench is entirely excluded from hearings held in closed session, which vastly exacerbates the insufficiency of Parliamentary oversight.

Greens' Senator Nick McKim made the following comments in 2016:[28]

---

[26] See, for instance, Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, 1.

[27] J Faulkner, "Surveillance, Intelligence and Accountability: an Australian story", 24 October 2014.

[28] N McKim, 'Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015', Senate, Debates, 13 October 2016, 1722–26, moving an amendment to Senator Penny Wong's *Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015* (Cth) that would see one seat on the PJCIS occupied by a member of the crossbench.

> *Neither party when in opposition want to appear weak on national security, so they fall into zombie lockstep with whoever is in government at the time and develop a bipartisanship that means legislation which is continually brought into this place … and which erodes some of our fundamental civil and human liberties in this country is not adequately scrutinised. We believe we need more scrutiny; we believe there needs to be more justification put before the Australian people for this continued erosion of their civil liberties in the name of counterterrorism and national security; and we believe a crossbench senator, as a member of the Joint Committee on Intelligence and Security, could play that role or be part of playing that role. This is a closed shop committee open only to members of the political duopoly in this country, and frankly the Australian people deserve better.*

Similar sentiments have been expressed by MPs across the political spectrum on the crossbench, including Senator Nick Xenophon[29] and Senator David Leyonhjelm.[30]

The HRLC believes that two crossbench members would add a diversity of opinion and critical voice to matters of national security that is sorely needed.

Recommendation 4:

The membership of the Parliamentary Joint Committee on Intelligence and Security should be changed so that it includes at least two members from the crossbench.

4.5 Judicial oversight

The current laws are varied and complex with respect to judicial oversight of intelligence agencies' functions, and detailed review goes beyond the remit of this submission except to provide some brief illustrative examples.

The HRLC notes that there is significant uncertainty as to whether the courts can adequately review Australian Security and Intelligence Organisation (**ASIO**) activities as a result of the difficulties associated with adducing evidence on intelligence gathering.[31] This includes the review of an adverse security assessment, which is regarded practically impossible given ASIO's ability to withhold the information on which it relied from the applicant and the court.[32]

[29] N Xenophon, 'Second reading speech: Parliamentary Joint Committee on Intelligence and Security Amendment Bill 2015', Senate, Debates, 13 October 2016, pp. 1729–32.

[30] D Leyonhjelm, *ABC News*, published 17 June 2018, accessed 28 November 2018, available at https://www.youtube.com/watch?v=L2a8PreUGt8.

[31] G.L Rose and D Nestorovska, "Terrorism and national security intelligence laws: assessing Australian reforms" [2005] *LAWASIA J* 127, 138, citing *Church of Scientology Inc v Woodward* (1982) 154 CLR 25.

[32] Australian Human Rights Commission, *Independent Review of the Intelligence Community Submission*, April 2011, 6.

Further, the use of judges as "Issuing Authorities" to oversee the execution of warrants that give extraordinary coercive powers to ASIO and Australian Federal Police officers has been criticised as "giving the veneer of judicial approval to a process which is in fact controlled by the executive".[33]

The HRLC is also concerned that no warrant or judicial supervision is required for ASIO and other Government agencies to access metadata retained under the *Telecommunications (Interception and Access) Act 1979* (Cth) (with the exception of journalists). This is a troubling and unjustified departure from the requirement that surveillance only be undertaken upon the grant of a judicial warrant. The recent comments of the European Court of Human Rights on the UK's illegal mass interception of communications are a timely reminder:[34]

> *[I]n view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.*

Finally, as an ancillary component of judicial oversight, we raise concerns as to the breadth of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), which can restrict accused persons and their defence lawyers from accessing evidence on grounds of national security.

The HRLC recommends that the Review conduct a comprehensive assessment of where judicial oversight is lacking, and recommend that it be strengthened accordingly.

Recommendation 5:

The Review should conduct a comprehensive assessment into where judicial oversight is lacking, and recommend that it be strengthened accordingly.

4.6 Protection of whistleblowers

The more information that the Government withholds, the more important whistleblowers are to ensuring transparency and accountability on matters of public interest. George Williams and Keiran Hardy have described whistleblowers as a "release valve" in a system that almost entirely prevents public scrutiny of the operations of intelligence agencies.[35] However, as raised above, the broad exemptions for intelligence information in the PIDA mean that the scheme does not provide any greater accountability than the IGIS already provides. There is no avenue for persons to raise matters of illegality, maladministration or breaches of human rights with a journalist or a Member of Parliament in the public interest.

[33] L Burton, N McGarrity and G Williams, "The Extraordinary Questioning and Detention Powers of the Australian Security Intelligence Organisation", (2012) 36 *MULR* 415, 429.

[34] *10 Human Rights Organisations and Others v United Kingdom* (ECHR, First Section, applications nos. 58170/13, 62322/14, 24960/15, 13 September 2018), [307].

[35] K Hardy, G Williams, "Executive Oversight of Intelligence Agencies in Australia" in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, ed. Z Goldman and S Rascoff, (Oxford University Press, New York, 2016), 339.

Australian and foreign whistleblowers have revealed shocking abuses of human rights by Western governments under the pretence of protecting national security. We know that former Prime Minister John Howard led our country into war with Iraq on weak intelligence because former Office of National Assessment officer Andrew Wilkie was willing to risk his career to reveal the truth. We know that UK and US intelligence agencies were facilitating indiscriminate surveillance of Australian citizens because Edward Snowden decided to risk his freedom in order to tell the public. Former Australian Secret Intelligence Service (**ASIS**) officer Witness K and his lawyer Bernard Collaery's decision exposed the Australian Government's immoral spying operation under which ASIS officers, reportedly posing as aid workers, entered East Timor and bugged the tiny, poor nation's cabinet rooms so to give Australia an advantage in sensitive negotiations over billions of dollars' worth of oil and gas resources.

Each of these disclosures was undeniably in the public interest. However, because no safeguards for external disclosures exist, Australian whistleblowers who expose misconduct by national security agencies can be investigated, prosecuted and potentially imprisoned; not because they endangered national security, but because they embarrassed the government.

This situation is worsening with new offences and harsher penalties for disclosing intelligence information. To identify just a couple,[36] the EFI Act introduced new offences for Commonwealth officers who communicate or otherwise deal with intelligence information and security classified information, attracting between three and seven years imprisonment. Journalists and others captured by the incredibly broad "espionage" offence face life in prison. Under section 35P of the ASIO Act, disclosing information relating to a "special intelligence operation" attracts a five year sentence.

This situation is entirely untenable in a democracy and undermines the confidence that the Australian public have in intelligence agencies. To address this, the HRLC previously submitted to the Statutory Review of the Public Interest Disclosure Act conducted by Philip Moss AM that:[37]

(a) the PIDA should explicitly protect disclosures that reveal violations of human rights, or that would promote accountability for such violations; and

(b) disclosures of serious violations of human rights be included within the "emergency disclosures" provisions, where the other relevant criteria for emergency disclosures are met.

The HRLC also recommended that an independent mechanism be empowered to:

(a) examine and where appropriate authorise the disclosure of intelligence information, balancing the public interest in the disclosure against any national security risks;

(b) resolve whether external disclosures may be made in the public interest under the protection of the PIDA in cases where:

(i) an internal disclosure or disclosure to IGIS has been made and has been elevated to the attention of the relevant Minister, the Speaker of the House of Representatives or the President of the Senate; and

(ii) the subject of the disclosure has not been resolved to the satisfaction of the potential whistleblower within a reasonable period of time.

[36] In its 2009 report, the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, with many of the provisions creating criminal offences for breaches: Australian Law Reform Commission, Secrecy and Open Government in Australia, Report No 112 (2009).

[37] Human Rights Law Centre, *Submission in relation to the Statutory Review of the Public Interest Disclosure Act*, 2 March 2016.

Recommendation 6:

There should be an avenue for external disclosures of intelligence information that do not pose a risk to national security and serve the public interest. Further, that harsh penalties for whistleblowers and journalists be repealed.

4.7 Freedom of information

The wholesale exemption of intelligence agencies from the *Freedom of Information Act 1982* (Cth) (**FOI Act**) is another unacceptable bar to public accountability.

The Office of the Australian Information Commissioner (**OAIC**) recently recommended that all intelligence agencies be subject to the operation of FOI legislation. Consistent with all other Australian Government departments and agencies, specific exemptions of the FOI Act would then provide appropriate protections for information held by intelligence agencies. As explained by the OAIC, exemptions should be "applied on a document-by-document basis to allow a nuanced approach to managing appropriate information disclosure".[38]

The definition of national security as a ground for refusing an FOI application should be reviewed and narrowed.[39]

Recommendation 7:

The Freedom of Information Act should apply to all intelligence agencies.

5. The concept of "national security" is not confined to the security of our nation

5.1 Concept of "national security"

Sections 6, 6B and 7 of the IS Act outline the functions of the ASIS. Subsection 11(1) limits intelligence agencies' functions as follows:

> *The functions of the agencies are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.*

[38] J McMillan and J Popple, *Submission to the Hawke Review: Review of freedom of information legislation*, Office of the Australian Information Commissioner, December 2012, [160].

[39] See Digital Rights Watch, *The State of Digital Rights*, May 2018, 8.

Causing harm to Australia's "economic relations" with another country is also an element of the new sabotage and espionage offences created by the EFI Act. As Australian Lawyers for Human Rights submitted to the PJCIS, this definition is "unworkably vague and will have an unreasonably chilling impact on freedom of speech and discourse regarding matters of genuine public interest".[40]

Given the extraordinary powers and protections that are accorded to intelligence and security agencies under the mandate of protecting Australia's national security, it is inappropriate and worrying that the definition is so broadly worded to include "Australia's national economic well-being".

5.2 Historical context of "economic well-being"

The phrase "Australia's national economic well-being" is very broad and not further defined in the relevant national security legislation. It appears the phrase first emerged in the original IS Act, which was the first attempt to form a legislative basis for the Australian Secret Intelligence Service (**ASIS**).

The *Intelligence Services Bill 2001* (Cth) (**IS Bill**) was introduced by then Foreign Affairs Minister Alexander Downer following the Samuels and Codd Royal Commission,[41] which was responding to claims that ASIS was not sufficiently accountable. According to the report, ASIS was modelled on its UK counterpart, the functions of which were to provide "foreign intelligence in furtherance of the Government's foreign, defence, security and economic policies". Samuels and Codd drafted a bill, which has not been made publicly available, but it seems reasonable to assume that this is where the drafting of subsection 11(1) originated.

Neither the explanatory memorandum to the IS Bill nor the Minister's Second Reading Speech expand on or meaningfully refer to the definition of "Australia's national economic well-being".

Helpfully, the Bills Digest[42] to the IS Act does provide some historical context to the provision:

> *…the phrase 'national economic well-being' is not defined. It would seem to include intelligence of economic significance to Australian governments. It may even include intelligence of commercial significance to Australian companies. The importance of economic intelligence has been increasingly recognised by ASIS and the Government. For example, in 1977 the First Hope Royal Commission observed:*
>
> > *In the past, intelligence has been believed to be of most relevance in the field of defence and related policy areas. It is, however, not only a matter of defence. More and more, intelligence is relevant to the formation of national policies in a number of other areas; this is a trend that will continue.*
>
> *On the recent Sunday program on DSD it was observed that 'now that the cold war is over the focus now is towards economic intelligence' and that 'all countries have to re-examine their traditional relationships because in the world of economic competitiveness countries no longer have allies, they only have interests'.*

It is clear that intelligence gathering, as conceived at the time, was not limited to threats to the Australian economy that had national security implications, but extended to Australia's national economic advancement.

---

[40] B Coyne, *Submission to the Parliamentary Joint Committee on Intelligence and Security on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017*, 22 January 2018, 5.

[41] Commission of Inquiry into the Australian Secret Intelligence Service, *Report on the Australian Secret Intelligence Service*, March 1995, [3.21].

[42] Department of Parliamentary Services (Cth), *Bills Digest*, No 11 of 2001, 27 June 2001.

This is consistent with more recent national security legislation. In the context of the EFI Act, the Replacement Explanatory Memorandum refers to "grave threat[s] to Australia's economic stability and well-being",[43] but later describes the definition of national security in far broader terms:[44]

> *Subparagraph 82.7(d)(ii) refers to harm or prejudice to Australia's economic interests. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's economic interests or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's economic interests. The prejudice to Australia's economic interests is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect on Australia's overall economy.*

5.3 How "economic well-being" has been explained by intelligence agencies

When asked about the meaning of the phrase "economic well-being", and why it is necessary, officers from intelligence agencies have not been able to articulate a satisfactory answer. They provide examples of grave economic risk such as major cyberattacks[45] without properly acknowledging the extent of activities that are, or that might be carried out under this definition.

In 2014, previous IGIS Dr Vivienne Thom was asked to explain the test for when ASIS' activities were for the national economic well-being, as opposed to the well-being of companies. Dr Thom's response was concerning: she indicated that there was no clear definition or limit to the power as it was determined by reference to the Government's requirements as set by the National Security Cabinet of Cabinet. She identified no outer limits, merely stating that "national economic well-being is a broad umbrella … and there are many areas of intelligence collection that could fall under it."[46]

5.4 How "economic well-being" has been applied by intelligence agencies

For the public to have confidence in our national security and intelligence agencies, it is vital that there is transparency and certainty around the coercive and intrusive powers granted to them. Yet, little information as to what operations this phrase has been used to justify has made it into the public. The few instances we do know about paint a disturbing picture.

It was apparently in the pursuit of "Australia's national economic well-being" that the Australian Government spied on East Timor to give it an advantage over its poor neighbour during oil and gas treaty negotiations.

---

[43] Explanatory Memorandum, *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), [3].

[44] Explanatory Memorandum, *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), [388].

[45] G McDonald, Estimates, Legal and Constitutional Affairs Legislation Committee, 25 May 2011, 124.

[46] V Thom, Estimates, Finance and Public Administration Legislation Committee, 26 May 2014, 176. See also similar response by the Office of the Inspector-General of Intelligence and Security, Response to question on notice taken before the Senate Finance and Public Administration Legislation Committee, 13 April 2017.

Alarmingly, national security powers have also been used against the Government's critics at home. In 2012, Attorney-General Nicola Roxon admitted that ASIO and the Australian Federal Police were spying on environmentalists.[47]

It is not clear what statutory powers ASIO officers use to gather intelligence domestically on these occasions. It may have been via section 19A of the ASIO Act, which is to be read with sections 17(1)(f) and 20. On their terms they may authorise ASIO to engage in activities in support of all of ASIS' functions including those unrelated to security as defined in the ASIO Act. Thus, through section 19A, ASIO's powers to gather intelligence domestically may be combined with ASIS' functions serving Australia's national economic well-being to allow for domestic surveillance. Regardless, protecting economic interests was clearly the aim of the operations, having been publicly justified on the basis of "major trade and investment implications" posed by protestors.[48]

These instances are likely just the tip of the iceberg, yet we may never find out the full extent to which spying has been carried out on Government dissidents and our neighbours. This is a deeply troubling aspect of Australia's national security legislation that must be rectified.

Recommendation 8:

The functions of the Australian Secret Intelligence Service should be clarified and narrowed as they relate to national economic well-being. The functions of the Australian Security Intelligence Organisation should be reviewed so as to exclude functions related to national economic wellbeing and should explicitly be limited to protect Australians' freedoms of expression, association and assembly.

[47] C Hamilton, "Is spying on anti-coal activists just the tip of the iceberg?" *The Conversation*, 4 June 2014.

[48] P Dorling, "ASIO eyes green groups" *The Sydney Morning Herald*, 12 April 2012.