THE *RICHARDSON REVIEW*: REVIVING THE 'PURPOSE' OF LAW ENFORCEMENT AND INTELLIGENCE LEGISLATION

BRENDAN WALKER-MUNRO*

This article examines Australia's recent review of its federal national security and intelligence agencies. The article argues that Australia's current legislative structure for its intelligence agencies unacceptably blurs the lines between intelligence and law enforcement in a number of areas. In seeking to make several recommendations for law reform, this article engages with the 'purpose' of that legislation, and builds on the Richardson Review to provide for better distinction between the officers of intelligence agencies ('spies') and law enforcement ('cops').

> William Roper: 'So, now you'd give the Devil benefit of law!'
>
> Sir Thomas More: 'Yes. What would you do? Cut a great road through the law to get after the Devil?'
>
> William Roper: 'Yes, I'd cut down every law in England to do that!'
>
> Sir Thomas More: 'Oh? And when the last law was down, and the Devil turned round on you – where would you hide, Roper, the laws all being flat? This country's planted thick with laws, from coast to coast – Man's laws, not God's – and if you cut them down – and you're just the man to do it – d'you really think you could stand upright in the winds that would blow then? Yes, I'd give the Devil benefit of law, for my own safety's sake.'[1]

On 30 May 2018, the Commonwealth Attorney-General commissioned the *Comprehensive Review of the Legal Framework of Australia's National Intelligence Community* ('*Richardson Review*').[2] Undertaken by Mr Dennis Richardson AC and building on the work completed by the *Independent Intelligence Review* in 2017 ('*2017 Review*'),[3] the *Richardson Review* was one of the largest and most significant examinations of Australia's intelligence and national security apparatus to ever be undertaken.

---

* Law and the Future of War Research Group, TC Beirne School of Law, The University of Queensland.

1 Robert Bolt, *A Man for All Seasons* (Vintage International, 1962) 66.

2 Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) ('*Richardson Review*').

3 Michael L'Estrange and Stephen Merchant, *2017 Independent Intelligence Review* (Report, June 2017).

The *2017 Review* already made a number of recommendations in relation to the National Intelligence Community ('NIC'), including the statutory establishment of the Office of National Intelligence, improved oversight and regulatory mechanisms, and increases to staffing. Relevant to this article, the *2017 Review* also recommended 'a comprehensive review of legislation', by an eminent and suitably qualified individual, to give clarity to 'a crowded suite of intelligence legislation'.[4] It was following that recommendation that Richardson – a former Director-General of the Australian Security Intelligence Organisation ('ASIO'), Secretary of the Department of Foreign Affairs and Trade, and Secretary of the Department of Defence – was appointed to conduct that review.

The *Richardson Review* was also conducted against a backdrop of a highly volatile, constantly fluctuating threat environment in which the dangers of cybercrime and foreign influence were at an all-time high.[5] The *Final Report*, released publicly on 4 December 2020, contained over 1,300 pages across four volumes and made 204 recommendations to government about the structure, legislation, and powers of Australia's NIC agencies.[6] What set the *Richardson Review* apart from preceding reviews was the sheer size and complexity of both the subject matter and the *Final Report*. Writing on the results of the *Richardson Review*, Ananian-Welsh said:

> In the 19 years since the terror attacks of September 11, 2001, federal parliament has introduced 124 separate acts concerning the national intelligence community. On the whole, these acts have enhanced government power, increased secrecy, and scrambled to keep up with a constantly evolving threat environment. The result is one of the most complex legislative landscapes in the world.[7]

This complex legislative landscape is spread across more than 2,000 pages of legislation in 14 Acts being utilised or deployed through the actions of 10 agencies.[8]

---

4 Patrick F Walsh, 'Transforming the Australian Intelligence Community: Mapping Change, Impact and Challenges' (2021) 36(2) *Intelligence and National Security* 243, 249, 252 <https://doi.org/10.1080/02684527.2020.1836829>. See also Jake Dudley, 'Critical Review of Intelligence Issues and Recommendations Relevant to the Next Defence White Paper' (2021) 29(1) *Journal of the Australian Institute of Professional Intelligence Officers* 10.

5 Australian Security Intelligence Organisation, *Annual Report 2021–22* (Report, 13 September 2021) 4; Sarah Kendall, 'Espionage Is Set to Overtake Terrorism as Australia's Top Security Concern: Are Our Anti-Spy Laws Good Enough?', *The Conversation* (online, 8 December 2021) <https://theconversation.com/espionage-is-set-to-overtake-terrorism-as-australias-top-security-concern-are-our-anti-spy-laws-good-enough-170462>.

6 'Comprehensive Review of the Legal Framework of the National Intelligence Community', *Attorney-General's Department* (Web Page, 4 December 2020) <https://www.ag.gov.au/national-security/consultations/comprehensive-review-legal-framework-governing-national-intelligence-community>.

7 Rebecca Ananian-Welsh, 'National Security Review Recommends Complete Overhaul of Electronic Surveillance: But Will It Work?', *The Conversation* (online, 4 December 2020) <https://theconversation.com/national-security-review-recommends-complete-overhaul-of-electronic-surveillance-but-will-it-work-151462>.

8 Including, but not limited to, the *Australian Border Force Act 2015* (Cth), *Australian Crime Commission Act 2002* (Cth) ('*ACC Act*'), *Australian Federal Police Act 1979* (Cth) ('*AFP Act*'), *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), *Australian Security Intelligence Organization Act 1979* (Cth) ('*ASIO Act*'), *Inspector-General of Intelligence and Security Act 1986* (Cth), *Independent National Security Legislation Monitor Act 2010* (Cth), *Intelligence Services Act 2001* (Cth) ('*IS Act*'), *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), *Office of*

Within such a framework, the *Richardson Review* found that many of the activities undertaken by NIC agencies are functionally undistinguishable from autocratic or tyrannical governments, such as intrusive surveillance, unexplained detention, secrecy, manipulation, and deceit.[9]

Therefore, the legislative framework of the NIC remains of fundamental importance, with relevance to the distinction between 'spies' – that is, the officers of NIC agencies vested with intelligence roles related to national security – and 'cops' – that is, members of law enforcement agencies seeking to investigate and prosecute criminal offences.

Stewart Baker first used these terms to describe a paradigm of separation between the purpose and powers of law enforcement and intelligence agencies in the United States ('US').[10] The genesis for this separation arose from the development of the US Federal Bureau of Investigation ('FBI') and the Central Intelligence Agency ('CIA') in the post-war 1940s. CIA agents had no police powers – such as arrest or subpoena – and the CIA was required to turn over all intelligence on domestic threats to the FBI.[11] The rationale there was simple – Americans did not need, or want, a 'secret police' agency mirroring the Gestapo (short for *Geheime Staatspolizei*, or Secret State Police) that accrued such infamy in Germany in World War II. Thus the spies-versus-cops paradigm reflected a very real desire to separate intelligence collection from criminal investigation.

However, scholars have now come to recognise that the spies-versus-cops paradigm is becoming less fit for purpose.[12] In the US, a rash of defections from the CIA (such as Aldrich Ames and Harold Nicholson) and the arrest of Fawaz Yunis in the 1980s was followed by the 'calamitous' failure of US intelligence to foreshadow the events of 9/11.[13] These events brought legislative change that permitted the FBI to task the CIA with intelligence gathering and gave the CIA imprimatur to investigate allegations of domestic espionage.[14]

Perhaps what is needed then – and what this article will propose – is a contemporary examination of Baker's question – 'should spies be cops?'.[15] Thus this article has three purposes, pursued in three parts. Part II will draw scholarly

---

National Intelligence Act 2018 (Cth), *Surveillance Devices Act 2004* (Cth) ('*SDA*'), *Telecommunications (Interception and Access) Act 1979* (Cth), and various offences arising under the *Crimes Act 1914* (Cth) and the *Criminal Code Act 1995* (Cth) ('*Criminal Code*').

9 *Richardson Review* (n 2) vol 1, 163–4, citing Michael Kirby, 'Australia's National Intelligence Community: Legislation, Principles of Efficiency and Legality and Considerations of Liberty and Democracy' (Speech, Consultative Workshop, 1 April 2019).

10 George Browder, *Hitler's Enforcers: The Gestapo and the SS Security Service in the Nazi Revolution* (Oxford University Press, 1996) <https://doi.org/10.1093/acprof:oso/9780195104790.001.0001>.

11 Stewart Baker, 'Should Spies Be Cops?' (1994) 97 (Winter) *Foreign Policy* 36, 36 <https://doi.org/10.2307/1149438>.

12 Arthur S Hulnick, 'Intelligence and Law Enforcement: The "Spies Are Not Cops" Problem' (1997) 10(3) *International Journal of Intelligence and CounterIntelligence* 269 <https://doi.org/10.1080/08850609708435350>; Daniel Richman, 'Prosecutors and Their Agents, Agents and Their Prosecutors' (2003) 103(4) *Columbia Law Review* 749; Fred F Manget, 'Intelligence and the Criminal Law System' (2006) 17 *Stanford Law & Policy Review* 415.

13 Hulnick (n 12) 281–4.

14 Ibid.

15 Baker (n 11).

attention to the *Richardson Review*, but also examine some of the critical findings of the *Richardson Review* in the context of the purposes of law enforcement and intelligence. Despite the significance of the *Richardson Review*, it has not had the benefit of a strong academic assessment since its publication. Part III will use the *Richardson Review* and Baker's paradigm to examine Australia's approach to separating law enforcement and intelligence – proposing that the purpose of law enforcement should not be used to advance intelligence collection better pursued by intelligence agencies, and intelligence agencies should not be used to investigate or enforce the criminal law. Lastly, this article seeks to offer some critique of the *Richardson Review*'s recommendations around law reform from the viewpoint of clarifying the distinction between law enforcement and intelligence, and why some of the *Richardson Review* recommendations go too far and others not quite far enough.

I AUSTRALIA'S NIC AND THE *RICHARDSON REVIEW*

The NIC is a term prominently used in an earlier review in 2017 of Australia's intelligence functions conducted by Michael L'Estrange and Stephen Merchant.[16] The report of that review included a recommendation that the NIC be an umbrella term used to describe three broad clusters of Australian agencies responsible for intelligence collection and dissemination at the national level:[17]

(a) The six agencies comprising the Australian Intelligence Community ('AIC'), being the ASIO, Australian Signals Directorate ('ASD'), Australian Secret Intelligence Service ('ASIS'), Australian Geospatial-Intelligence Organisation ('AGO'), the Defence Intelligence Organisation ('DIO') and the Office of National Assessments (now the Office of National Intelligence ('ONI'));
(b) Federal criminal intelligence bodies such as the Australian Criminal Intelligence Commission ('ACIC') and the Australian Transaction Reports and Analysis Centre ('AUSTRAC'); and
(c) Federal law enforcement agencies, namely the Australian Federal Police ('AFP'), as well as the Border Force, Office of Transport Security and the Department of Immigration and Border Protection (now subsidiary organs of the Department of Home Affairs ('DoHA')).[18]

Most importantly for this article, the *2017 Review* also reinforced the fundamental importance of maintaining the dividing lines of purpose and power established by the *Royal Commission on Intelligence and Security* ('*Hope Royal Commission*') of the 1970s and 1980s between 'foreign and security intelligence,

16 L'Estrange and Merchant (n 3).

17 Cat Barker, 'Intelligence Community Reforms' (Briefing Book, Parliamentary Library, Parliament of Australia, July 2019) <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/ pubs/BriefingBook46p/IntelligenceCommunity>.

18 Though not a law enforcement agency, the Australian Security Intelligence Organisation ('ASIO') was also subsumed into Department of Home Affairs ('DoHA').

intelligence and law enforcement, intelligence collection and assessment, and intelligence assessment and policy formulation'.[19] These dividing lines, first promulgated by Hope J in the Royal Commission reports which helped establish agencies, like ASIO,[20] are also recognised in academia.[21]

In Australia, scholars have recognised the dissolution of barriers between law enforcement and intelligence agencies.[22] Even as the report of the earlier *2017 Review* was released – recommending the establishment of the ONI and coordinating transparent intelligence sharing across law enforcement agencies – the government created the 'super ministry' of the DoHA. The speed of the transition and subsequent structure of Australia's NIC led to questions about exactly what the purpose of the *2017 Review* was in the first place.[23]

The *Richardson Review* also noted this peculiar function of the NIC. Each of the agencies reviewed were said to have sought power for power's sake, with the observation that '[t]oo often, Australian agencies look over the fence and want what another agency has so that they can, effectively, do their own thing in isolation of others'.[24] This observation is perhaps the inverse outcome of Baker's original paradigm – law enforcement or intelligence agencies becoming overly jealous of the powers of their contemporaries, without properly contemplating the *purpose* for which those powers were given.

A The Importance of Purpose

In that context then, why does purpose matter? Purpose is crucial in both law enforcement and intelligence for two reasons: one, it guides how, when and why intrusive powers given to organs of the state may be used to lawfully violate the human rights of persons suspected of conduct harmful to the body politic; and second, it determines the boundaries within which such conduct is constrained by oversight bodies.[25]

After all, the purpose of intelligence agencies is to safeguard national security, inform top-level decision making and provide governmental awareness of threats

19 L'Estrange and Merchant (n 3) 6.

20 See also sections 11(2)(a) and (b) of the *IS Act* (n 8) which preclude *IS Act* agencies from engaging in policing or law enforcement functions.

21 William Funk, 'Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma: A History' (2007) 11(1) *Lewis & Clark Law Review* 1099; Danielle Keats Citron and Frank Pasquale, 'Network Accountability for the Domestic Intelligence Apparatus' (2010) 62(1) *Hastings Law Journal* 1441.

22 Kent Roach, 'The Eroding Distinction between Intelligence and Evidence in Terrorism Investigations' in Nicola McGarrity, Andrew Lynch and George Williams (eds), *Counter-Terrorism and Beyond: The Culture of Law and Justice after 9/11* (Routledge, 2010) 60–80; Greg Martin, 'Outlaw Motorcycle Gangs and Secret Evidence: Reflections on the Use of Criminal Intelligence in the Control of Serious Organised Crime in Australia' (2014) 36(3) *Sydney Law Review* 501.

23 Peter Edwards, 'Keeping Australians and Their Civil Liberties Safe: The Future of the Hope Model', *The Strategist* (online, 13 May 2020) <https://www.aspistrategist.org.au/keeping-australians-and-their-civil-liberties-safe-the-future-of-the-hope-model/>.

24 *Richardson Review* (n 2) vol 1, 42. Chapter 12 of the *Richardson Review* is given to exactly this issue.

25 Vincent Southerland, 'The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies' (2022) *UCLA Law Review* (forthcoming).

to the national interest.[26] The purpose of law enforcement is to identify, investigate and prosecute persons who offend against the criminal law of the state.[27] Therefore, the purpose for which information has been gathered becomes incredibly important – if the onus is on the state to prove contravention of the criminal law, then the onus also falls to ensure that evidence has been legally obtained and properly handled.

Purpose also matters from the perspective of oversight, which seeks to ensure that both powers entrusted to law enforcement and intelligence agencies are being used in accordance with the statutes that grant them, operations are conducted in accordance with good public policy, and prosecutions or administrative actions taken are done in good faith. Yet, oversight in Australia and elsewhere comes in different flavours dependent on the purpose of the agency. For example, the AFP is subject not only to civilian scrutiny by the Commonwealth Ombudsman but the probity of its officers are subject to the Australian Commission for Law Enforcement Integrity.[28] Intelligence agencies are generally more subject to parliamentary scrutiny,[29] however, the Inspector-General of Intelligence and Security (a statutory role) has been recently been given a broader mandate to oversee *Intelligence Services Act 2001* (Cth) ('*IS Act*') agencies.

The *Richardson Review* was one of the most comprehensive undertaken of Australia's NIC, but it is by no means the first. Including both of the *Hope Royal Commissions* in 1974–77 and 1983–84, as well as the *Richardson Review* itself, Australia's NIC has been reviewed eight times in 50 years.[30] These are perhaps the only ways for most members of the public to ever view the interior workings and functions of Australia's intelligence and law enforcement agencies, given most NIC agencies are exempt from the *Freedom of Information Act 1982* (Cth) in respect of their activities, and the law enforcement NIC agencies receive large swathes of exemptions over certain material.[31] Other agencies, such as DIO and ASD, are not required to publicly publish information about their functions or capabilities.[32]

---

26 Loch K Johnson, 'National Security Intelligence' in Loch K Johnson (ed), *The Oxford Handbook of National Security Intelligence* (Oxford University Press, 2010) 3, 7–23 <https://doi.org/10.1093/oxfordhb/9780195375886.003.0001>.

27 Vanda Felbab-Brown, 'The Purpose of Law Enforcement Is to Make Good Criminals? How to Effectively Respond to the Crime-Terrorism Nexus' (Speech, Potomac Institute for Policy Studies, 21 November 2013) <https://www.brookings.edu/on-the-record/the-purpose-of-law-enforcement-is-to-make-good-criminals-how-to-effectively-respond-to-the-crime-terrorism-nexus/>.

28 Tim Prenzler, 'The Evolution of Police Oversight in Australia' (2011) 21(3) *Policing and Society* 284 <https://doi.org/10.1080/10439463.2011.570866>; Tim Prenzler and Garth Den Heyer (eds), *Civilian Oversight of Police: Advancing Accountability in Law Enforcement* (CRC Press, 2016) <https://doi.org/10.1201/b19040>.

29 Andrew Defty, 'From Committees of Parliamentarians to Parliamentary Committees: Comparing Intelligence Oversight Reform in Australia, Canada, New Zealand and the UK' (2020) 35(3) *Intelligence and National Security* 367 <https://doi.org/10.1080/02684527.2020.1732646>; Patrick Walters, 'Spies, China and Megabytes: Inside the Overhaul of Australia's Intelligence Agencies' (2018) 4 *Australian Foreign Affairs* 27.

30 *Richardson Review* (n 2) vol 1, 86. Dennis Richardson also conducted an earlier review on the Australian Intelligence Community in 1991.

31 *Freedom of Information Act 1982* (Cth), ss 33, 37–8, schs 2, 3. The *Richardson Review* (n 2) did not seek to disturb these protections: at vol 4, 35–42.

32 Which the *Richardson Review* recommended be revisited: *Richardson Review* (n 2) vol 1, 298.

A key finding of the *Richardson Review* was that the Commonwealth legislative provisions for electronic surveillance needed to be urgently replaced with a modern-day version, labelling Australia's current telecommunications legislation 'a dog's breakfast'.[33] The *Richardson Review* identified significant harms that could arise from this patchwork area of law:[34]

(a) Firstly, the level of approval required and the matters to be considered by the authorising officer are wildly variant between the various Acts;
(b) Secondly, the inconsistency of the surveillance provisions leads to unnecessary administrative burdens on the intelligence and law enforcement agencies, which in turn runs the risk that they might inadvertently breach the law they are created to uphold; and
(c) Thirdly, the laws lack clarity such that individual members of the public might not know the reach and ambit of powers which interfere with their privacy and freedoms. Even in cases where a person is accused of the most heinous of crimes, they ought to retain the rights and protections of the law.[35]

The *Richardson Review* engaged with, and discarded, various alternatives to dealing comprehensively with modern electronic surveillance. The *Richardson Review* recommended dispensing with the ad hoc amendments to the telecommunications and surveillance acts that had typified legislative policy for the last 40 years. In making a recommendation for a unifying electronic surveillance Act, the *Richardson Review* was blunt about the work involved:

> Developing a new Act for electronic surveillance would be a significant undertaking. The work involved would exceed the scale of any previous national security legislative project – repealing and rewriting almost 1,000 pages of laws that enable and support critical investigations by Commonwealth, state and territory agencies on a daily basis …
>
> The fact that the electronic surveillance powers are both highly intrusive and vital for the purposes of serious investigations demands a legal framework that is clear, robust and internally consistent. Only a comprehensive reform of the electronic surveillance framework would achieve this objective.[36]

The *Richardson Review* also eschewed any attempts to bring the NIC together under a unifying legislative Act in a manner similar to New Zealand.[37]

Much of the criticism of the *Richardson Review* appears to be focussed on the failure to recommend adoption of the 'double lock' system for warrants or authorisations for activities that would ordinarily attract criminal liabilities.[38] A double lock system would require that warrants or authorisations for NIC agencies

---

33 *Richardson Review* (n 2) vol 1, 45.
34 Ibid vol 2, 250–62.
35 *R v Ul-Haque* (2007) 177 A Crim R 348, 378 [94]–[95] (Adams J) ('*Ul-Haque*').
36 *Richardson Review* (n 2) vol 2, 265–6. See also vol 2, ch 27.
37 The *Intelligence and Security Act 2017* (NZ) was enacted following a similar review to the *Richardson Review* (n 2), but the *Richardson Review* did not consider that the National Intelligence Community ('NIC') would benefit from a similar approach, as Australia's NIC is more numerous and more complex than their New Zealand ('NZ') counterparts: *Richardson Review* (n 2) vol 1, 372.
38 Peter Edwards, '*Richardson Intelligence Review* Recommendations Must Be Implemented – and Soon', *The Strategist* (online, 10 March 2021) <https://www.aspistrategist.org.au/richardson-intelligence-review-recommendations-must-be-implemented-and-soon/>.

are approved not only by the relevant Minister, but also by an independent scrutineer such as a judge or statutory appointment of the executive.[39] The *Richardson Review*'s apparent reticence to adopt a double lock system owes in large part to the 'gold standard' existence of impartial examining and oversight bodies in the Inspector-General of Intelligence and Security ('IGIS'), as well as the Independent National Security Legislation Monitor ('INSLM')[40] and Independent Reviewer of Adverse Security Assessments.[41] There exists at the time of writing no contemporary of the IGIS in any jurisdiction anywhere in the world.

Another factor contributing to the rejection of the double lock appears tied to the *Richardson Review*'s recommendation that the Attorney-General be the only Minister permitted to grant warrants and authorisations to the NIC, commensurate with their position as the Commonwealth's First Law Officer.[42] A rejection on that basis appears confusing. The *Richardson Review* considered all of the existing powers available to the NIC, many of which are authorised by the Attorney-General, but found that NIC agencies often viewed these legislative safeguards as an administrative burden or a hindrance to data sharing or operations.[43] The agencies almost unilaterally called for amendment to powers or even additional powers that were neither reasonably necessary nor acceptable for their purposes.[44] Again, not considering a double lock is difficult to square with the *Richardson Review*'s findings that NIC agencies 'lack appreciation of the careful balance that must be struck between an accused's right to a fair trial, the principle of open justice and the protection of national security information'.[45]

What public response to the *Richardson Review* has occurred has also been mixed. Some are cautiously optimistic given the scale and scope of the *Richardson Review*,[46] others are critical of the lack of parliamentary or judicial oversight recommended under the *Richardson Review* for intelligence and law enforcement activities.[47] A common theme to many of the responses has been that the *Richardson Review* was well and truly overdue but that the glacial pace of reform observed

---

39 Examples in the *Richardson Review* include the NZ Commissioner of Intelligence warrants under the *Intelligence and Security Act 2017* (NZ), the Information Commissioner under chapter 13 of the Canadian *Communications Security Establishment Act*, SC 2019, and a Judicial Commissioner appointed under the *Investigatory Powers Act 2016* (UK): *Richardson Review* (n 2) vol 1, 43–44 [18.39], 44–5 [18.42], 52 [18.75].

40 *Independent National Security Legislation Monitor Act 2010* (Cth) s 6.

41 A non-statutory role: 'Independent Reviewer of Adverse Security Assessments', *Attorney-General's Department* (Web Page) <https://www.ag.gov.au/national-security/independent-reviewer-adverse-security-assessments>.

42 *Richardson Review* (n 2) vol 1, 53.

43 Ibid vol 1, 34.

44 Ibid vol 1, 35.

45 Ibid vol 1, 59.

46 Ananian-Welsh (n 7); Edwards (n 38).

47 Law Council of Australia, '*Richardson Review*: Law Council Deeply Concerned by Recommendation to Cut Judiciary out of Warrant Approval' (Media Release, 4 December 2020) <https://www.lawcouncil.asn.au/media/media-releases/richardson-review-law-council-deeply-concerned-by-recommendation-to-cut-judiciary-out-of-warrant-approval>; Kym Bergmann, 'Criticism Mounts on *Richardson Review* of Intel Operations', *Asia-Pacific Defence Reporter* (online, 6 December 2020) <https://asiapacificdefencereporter.com/criticism-mounts-on-richardson-review-of-intel-operations/>; Kate Grayson and Anthony Bergin, 'Did

after the *Hope Royal Commission* (where some recommendations were not passed until four decades later) must be avoided.[48] The Law Council of Australia voiced its concerns that, despite submissions to the contrary, the *Richardson Review* did not recommend judicial oversight for intelligence warrants, concerns it has recently ventilated again in response to the DoHA discussion paper on the new electronic surveillance legislation.[49] Oversight from a broader perspective – by both statutory agencies and parliamentary committees – featured in those same submissions.[50]

The careful balance of collective security and individual security requires that the state retain primacy in the interference with basic rights. However, in doing so the state must accept responsibility and appropriately safeguard the proper and appropriate exercise of any such interference.[51] Thus below I discuss some of the more poignant findings of the *Richardson Review* and seek to repose Baker's question about the boundaries between spies and cops to focus on *purpose* as those powers relate to various interferences with rights and freedoms, and whether they provide the body politic of Australia with greater overall security and safety.

B Foreign Intelligence versus Security Intelligence

As the *Hope Royal Commissions* found and the *Richardson Review* confirmed, intelligence is both a product and a process. Intelligence may also be a tool of diplomatic policy – for backchannel communications, and exertion of foreign policy in ways that are either deniable by the government 'at large' or that are deceptive as to either intent or outcome. What shapes intelligence is the purpose for which it is sought.[52]

Foreign intelligence is directly defined under the *Australian Security Intelligence Organisation Act 1979* (Cth) as 'intelligence about the capabilities, intentions or activities of people or organisations outside Australia'.[53] This intelligence is directly tied to the legislated functions of ASIS, AGO, and ASD.[54] By comparison, security intelligence is a hybrid concept derived from the *ASIO Act* as intelligence relating to any combination of espionage, sabotage, politically motivated violence, acts against the Australian Defence Force ('ADF') or acts of foreign interference, the protection of Australia's territorial and border integrity, or Australia's security responsibilities to other countries.[55]

---

the *Richardson Intelligence Review* Get It Right?', *The Strategist* (online, 5 February 2021) <https://www.aspistrategist.org.au/did-the-richardson-intelligence-review-get-it-right/>.

48 Edwards (n 38).

49 Law Council of Australia, Submission to Department of Home Affairs, *Reform of Australia's Electronic Surveillance Framework: Discussion Paper* (18 February 2022) 33–4 <https://www.lawcouncil.asn.au/publicassets/892ec930-1595-ec11-944b-005056be13b5/4176%20-%20ESR%20DP.pdf>.

50 Ibid 38–45; Grayson and Bergin (n 47).

51 Max Weber, *Politics as a Vocation*, tr HH Gerth and C Wright Mills (Fortress Press, 1965).

52 *Richardson Review* (n 2) vol 1, 155–6.

53 *ASIO Act* (n 8) s 4 (definition of 'foreign intelligence').

54 *IS Act* (n 8) ss 6, 6B, 7.

55 *ASIO Act* (n 8) ss 4 (definition of 'security'), 17.

Obviously, there exists potential for substantial overlap between these two spheres. For example, consider a North Korean warship that leaves harbour with orders to attack Australian Navy vessels. The capability of that warship would be foreign intelligence within the remit of ASIS, AGO and ASD, whilst its orders – constituting an attack against the ADF – is more properly security intelligence. Nor does the legislation create any distinction between onshore and offshore intelligence activities: the intention and capabilities of the North Korean warship does not change substantially whether it is inside Australian territorial waters, or it is not. The *Richardson Review* highlights this disparity as crucial by referring to collection of intelligence on the activities of the Islamic State of Iraq and Syria,[56] but also highlighted that the agencies possess sufficient legislative scope to cooperate on matters where the spheres overlap.[57]

The separation of foreign and security intelligence, and onshore and offshore activities, is given statutory recognition by force of the legislative authorities for intelligence collection by Australian NIC agencies. By examining the various Acts (predominantly the *ASIO Act* and *IS Act*) which authorise, legalise and regulate such intelligence collection, it is possible to identify how and under what circumstances intelligence collection may be performed, on whom it may be performed, who it may be authorised by or alternately whether no such authorisation is needed. A summary of the process by which the *ASIO Act* and *IS Act* delineate these activities is shown in Table 1 on the next page.

Foreign intelligence about a non-citizen may not be gathered inside Australia without a warrant,[58] but ASIO retains primacy to conduct that warranted intelligence collection in Australia and may do so irrespective of whether the person is a citizen, permanent resident or otherwise.[59] The powers afforded to ASIO under the warrant regime are significant. A warrant may authorise the search of places, people, and things;[60] the search, interception, modification, or erasure data on a computer (no matter its location);[61] installation of optical, listening or tracking surveillance devices;[62] inspection or alteration of articles of post;[63] or apprehension ahead of compulsory questioning.[64]

56 *Richardson Review* (n 2) vol 1, 169. As the Islamic State of Iraq and Syria ('ISIS') is an organisation outside of Australia that impacts on Australia's national security interests, it is a legitimate foreign intelligence target. However, ISIS also represents a threat to Australian security interests and so is also a legitimate security intelligence target.

57 *Richardson Review* (n 2) vol 1, 197; *IS Act* (n 8) ss 6(1)(da), 7(1)(e); *ASIO Act* (n 8) s 17(1)(f).

58 Foreign intelligence is not permitted onshore in respect of Australian citizens or permanent residents: *ASIO Act* (n 8) s 27A(9).

59 Ibid divs 2–4.

60 Ibid s 25.

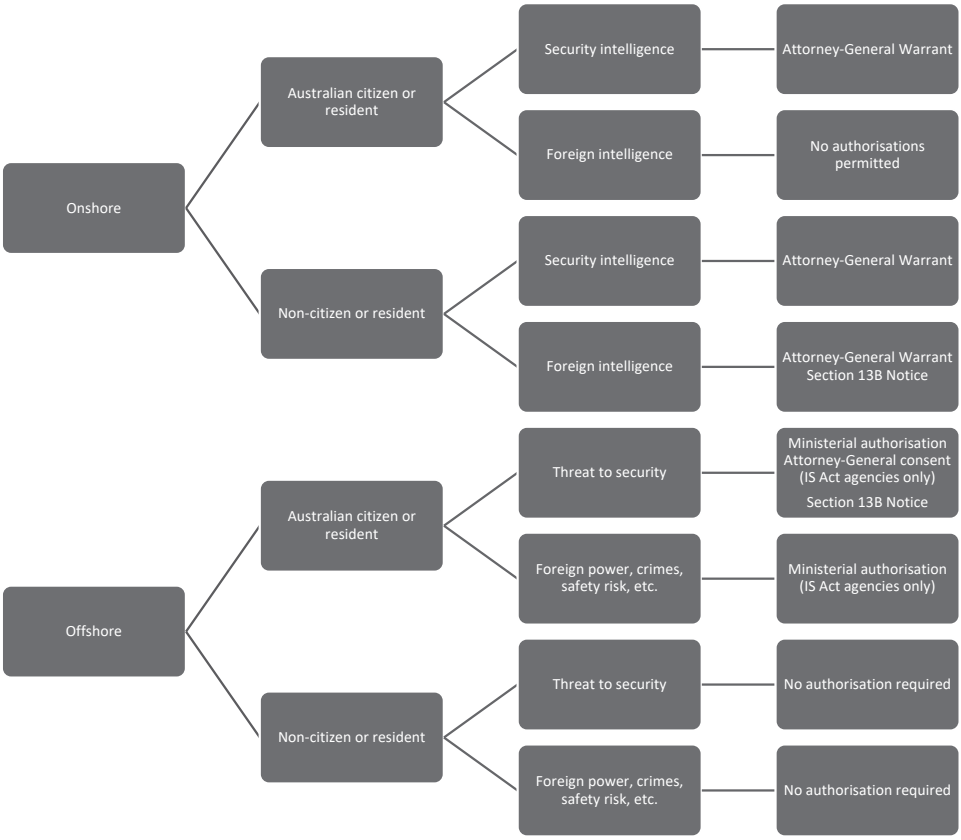
61 Ibid s 25A.

62 Ibid s 26.

63 Ibid ss 27, 27AA.

64 Ibid ss 34B, 34BD, 34BE. See also pt 2 div 3 sub-div C (for the ancillary powers available under a questioning warrant).

Table 1: Australia's Ministerial Authorisation and Warrant Scheme



Further, intelligence on an Australian person may not be generated by ASIS, AGO or ASD without an authorisation from the relevant Minister (the Foreign Minister for ASIS, and the Defence Minister for AGO or ASD).[65] To issue an authorisation, the Minister must be satisfied that the person is, inter alia, acting on behalf of a foreign power; engaging in activities likely to present a significant risk to a person's safety, prejudice the operational security of ASIS or involve the proliferation of weapons of mass destruction or prohibited goods; or is involved in a serious crime involving money, goods, or intellectual property.[66] This important safeguard was recognised because those agencies accept a 'higher degree of political risk when it authorises intrusive or covert collection against Australians' and that by required ministerial authorisation there existed 'a public assurance value in having a senior elected official make the decision to produce intelligence

65 *IS Act* (n 8) ss 8, 9.
66 Ibid s 9(1A)(a).

on an Australian'.[67] The *Richardson Review* made it clear that acting in the purposes of national security was not something susceptible to legislative mandate – given the evolutionary and fluid nature of threats to national security, the *Richardson Review* endorsed a regime that was inclusive by nature, and exculpatory by design.

Where an Australian poses a threat to security and is also located offshore, an IS agency also requires the authority of the Attorney-General in addition to that of the relevant Minister.[68] ASIO needs no such authority to generate security intelligence on such a person.[69] Rather than accepting the contention of ASIS that these additional requirements were unintentional, the *Richardson Review* underlined that these types of approval are legitimately required to allow the Attorney-General to disambiguate IS agency operations from those undertaken by ASIO (either warranted or unwarranted), and permits ASIO to discharge its statutory function to advise government on threats to security.[70] Instead, the *Richardson Review* recommended a change to sequencing only – that the authorisation of the Attorney-General be obtained first, then the relevant Minister. The benefit of this sequencing would enable the Attorney-General to consider all information (including the advice of ASIO) as to whether to agree to an *IS Act* agency authorisation.[71]

Equally, the possession of Australian citizenship or residency affects the intrusiveness to which *IS Act* agencies and ASIO may apply their powers. Australians may not be the subject of an onshore foreign intelligence warrant[72] but may be subject to foreign intelligence processes offshore (assuming the relevant ministerial authorisation is in force).[73] Non-Australians have no such safeguards. *IS Act* agencies may also continue to generate foreign intelligence on an Australian onshore, assuming they do so via lawful means that do not otherwise require a warrant, and the *Richardson Review* found that this ought to remain the case *except* in circumstances where an Australian onshore is acting under instructions of a foreign power.[74] This was because such a person would affect Australia's national interests, irrespective of whether they were onshore or offshore, and the prevalence of dual citizenships having increased since the *Hope Royal Commission*.[75]

---

67 *Richardson Review* (n 2) vol 1, 243–4. Cf the *IS Act* (n 8), which prima facie permits collection of intelligence on non-Australians without an authorisation or warrant, as this is consistent with those agencies' purposes.

68 *IS Act* (n 8) s 9(1A)(b).

69 Cf *ASIO Act* (n 8) s 17(1)(a). ASIO may also request the Australian Secret Intelligence Service assist in respect of that person: *IS Act* (n 8) s 13B.

70 *Richardson Review* (n 2) vol 1, 189.

71 Ibid vol 1, 194.

72 *ASIO Act* (n 8) s 27A(9). The *Richardson Review* also recommended that only the Attorney-General authorise *IS Act* (n 8) authorisations and *ASIO Act* (n 8) warrants: *Richardson Review* (n 2) vol 1, 312–18.

73 The *Richardson Review* made a strong recommendation that this process be adopted for ASIO, noting that no such scheme currently exists and therefore 'the *ASIO Act* currently provides no mechanism by which the Attorney-General or Minister for Home Affairs can assess the propriety, necessity, reasonableness and proportionality of ASIO's intelligence collection activities in respect of Australians offshore': *Richardson Review* (n 2) vol 1, 347.

74 Ibid vol 1, 241.

75 Ibid vol 1, 238–41.

Finally, the offshore condition is highly relevant for intelligence collection activities undertaken by NIC agencies. ASIS, for example, is Australia's predominant agency for conducting espionage against foreign states, without their consent and preferably without their knowledge. Whilst espionage is not per se illegal under international law, it is traditionally captured by the domestic legislatures of each state as a criminal offence, and undoubtedly will cause diplomatic tensions if detected.[76] Yet, covert intelligence generation by NIC agencies undoubtedly occurs offshore, without ministerial approval or control (with the perhaps ironic exception of ASIS, AGO and ASD, which must obtain ministerial authorisation to do so).[77]

Ultimately, the two regimes (authorisation and warrants) make uneasy but necessary bedfellows to protect the rights of Australians outside of Australia from intrusive foreign intelligence collection, compared to warranted security intelligence collection against all of those inside Australia's borders.

II HOW AUSTRALIA CURRENTLY DELINEATES LAW ENFORCEMENT AND INTELLIGENCE

The collective effect of Australia's national security legislation is intended to place specific boundaries to what can (and perhaps more importantly, cannot) be done by spies and by cops in the pursuit of their duties. When ASIO can issue security assessments that determine whether a person remains resident in Australia or obtains employment,[78] and when the AFP or ACIC may obtain warrants to covertly intercept phone calls and text messages, the boundaries of these agencies' conduct have significant real-world consequences. Therefore, agencies of the executive – including the NIC – must have legislative authorisation for the activities they pursue. If they do not, they rightly face liability under the law irrespective of the nobility of their intentions.[79]

There is more substance to the argument on discriminating between the role of spies and cops in a modern, liberal democracy. In essence, the focus of my argument is on the purpose for which powers are being exercised and conduct is being engaged in. The Law Council of Australia submissions to the *Richardson Review* highlighted that not only did the distinction between law enforcement and intelligence purposes encourage agencies not to duplicate effort (thereby wasting

76 See A John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28(3) *Michigan Journal of International Law* 595; Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) *Chicago Journal of International Law* 353; Iñaki Navarrete and Russell Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions' (2019) 51(4) *Cornell International Law Journal* 897.

77 Without imposing such a restriction, the *Richardson Review* has recommended that the Department of Foregin Affairs and Trade and/or the Foreign Minister be appraised of such activities to manage the international relations risks arising from same: *Richardson Review* (n 2) vol 1, 356.

78 Ibid vol 4, ch 44; *ASIO Act* (n 8) pt IV.

79 *Entick v Carrington* (1765) 19 St Tr 1030; 95 ER 807; *A v Hayden [No 2]* (1984) 156 CLR 532; *Ridgeway v The Queen* (1995) 184 CLR 19.

resources), but ensured the agencies performed their unique roles separately under clear, transparent schemes consistent with human rights and the rule of law.[80] Merging the purposes of law enforcement and intelligence runs a very real risk of creating an autocratic surveillance body that covertly collects information without any judicial or public oversight, whilst potentially permitting that evidence to be used against a witness without their knowledge.[81]

Describing exactly that hypothetical world, in 1925 Franz Kafka wrote:

> … the legal records of the case, and above all the actual charge-sheets, were inaccessible to the accused and his counsel, consequently one did not know in general, or at least did not know with any precision, what charges to meet in the first plea; accordingly it could be only by pure chance that it contained really relevant matter. … In such circumstances the Defence was naturally in a very ticklish and difficult position. Yet that, too, was intentional. For the Defence was not actually countenanced by the Law, but only tolerated, and there were differences of opinion even on that point, whether the Law could be interpreted to admit such tolerance at all.[82]

Nearly 100 years later, the *Richardson Review* has found that the distinction between cops and spies remains 'as relevant today as when the concept was originally considered'.[83]

That is not to say that this article advocates for silos between law enforcement and intelligence, nor that one should work ignorant of the other. In the highly volatile and complex security environment of Australia, and with the rise of non-state threats, cooperation and coordination have become more important than ever. In particular, the coordination of intelligence and law enforcement agencies comes into sharp focus when dealing with matters of cyber-crime and cyber-enabled crime: offences that can be transnational in character and difficult to attribute to individuals, states or non-state actors until well after the event (a concept the *Richardson Review* was keen to engage with). What remains important is that intelligence agencies and law enforcement ensure they remain mindful of the purpose (and therefore, the legality) of their collection, analysis, investigation and disruption activities.

A Collection of Intelligence versus Enforcement of the Criminal Law

An issue blurring the lines between law enforcement and intelligence gathering arises in the consideration of criminal intelligence. The AFP and DoHA operate and maintain a comprehensive criminal intelligence practice framework that governs collection of information both domestically and overseas.[84] Under that

80 *Richardson Review* (n 2) vol 1, 270.

81 The *Richardson Review* cited Canada's Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police as an example of Canada's security and law enforcement systems suffering from exactly this form of illegality: *Richardson Review* (n 2) 272.

82 Franz Kafka, 'The Trial', tr Willa Muir and Edwin Muir in Willa Muir and Edwin Muir (eds), *The Complete Novels: The Trial, America, The Castle* (Vintage, 1999) 11, 69–70, cited in *Roberts v Parole Board* [2005] 2 AC 738, 787 [95] (Lord Steyn).

83 *Richardson Review* (n 2) vol 1, 275.

84 Australian Criminal Intelligence Commission, *Australian Criminal Intelligence Management Strategy 2017–2020* (March 2017) ('*ACIMS*').

framework and consistent with Australian law, the investigation and enforcement of Australia's criminal law for Commonwealth offences will fall in the ordinary course to the AFP.[85] In addition, the AFP is vested with a function to provide policing services (such as investigating said offences) to Australia's intelligence and security agencies.[86]

However, certain authorisations and warrants available to the *IS Act* agencies and ASIO have the collective effect of also permitting the collection of intelligence on criminal activity. For example, an *IS Act* agency may obtain a ministerial authorisation to obtain foreign intelligence on an Australian person engaging in conduct that involves the proliferation of weapons of mass destruction, contravention of a UN sanction enforcement law,[87] or the commission of a serious crime 'by moving money, goods or people … using or transferring intellectual property … transmitting data or signals by means of guided and/or unguided electromagnetic energy'.[88] An ASIO warrant may also be sought in respect of persons engaging in activities associated with inter alia politically motivated violence[89] or acts of foreign interference[90].

When compared side-by-side, there are significant differences between the policing powers of the AFP and the intelligence gathering powers of the AIC agencies, in circumstances where those agencies may be pursuing the same conduct. For example, search and arrest warrants under the *Crimes Act 1914* (Cth) with respect to criminal offences are issued by a judicial officer,[91] whilst those issued under the *IS Act* or *ASIO Act* are signed by officers of the Executive.[92] This means that NIC agencies may obtain information subject to an intelligence process that subsequently becomes evidentiary for a criminal prosecution.

Such a danger is more pronounced in circumstances where the AFP then seeks to lead such evidence in prosecution. The intelligence may have been generated

---

85 *AFP Act* (n 8) ss 4 (definition of 'police services'), 8(1)(b). In certain cases, border or transnational offences will be investigated by DoHA (such as maritime breaches, smuggling, customs offences, or drugs).

86 Ibid s 8(1)(bf)(ii).

87 Given effect by the *Charter of the United Nations Act 1945* (Cth) s 2B; *Charter of the United Nations (UN Sanction Enforcement Law) Declaration 2008* (Cth) sch 1, as amended by *Charter of the United Nations (UN Sanction Enforcement Law) Amendment Declaration 2021 [No 1]* (Cth).

88 *IS Act* (n 8) ss 9(1A)(a)(iv)–(vii). The *Richardson Review* explicitly declined to collapse this provision down to relate to 'serious crime' as this would expand the authorisation to cover any criminal offence punishable by 12 months imprisonment or more: *Richardson Review* (n 2) vol 2, 106–8.

89 Including offences under: *Criminal Code* (n 8) div 72 sub-div A, div 119, pt 5.3; *Crimes (Hostages) Act 1989* (Cth); *Crimes (Ships and Fixed Platforms) Act 1992* (Cth); *Crimes (Aviation) Act 1991* (Cth); *Crimes (Internationally Protected Persons) Act 1976* (Cth). See also *ASIO Act* (n 8) ss 4(ba)–(d) (definition of 'politically motivated violence').

90 Though defined in section 4 of the *ASIO Act*, these provisions have significant overlap with the provisions inserted in division 92 of the *Criminal Code*.

91 *Crimes Act 1914* (Cth) ss 3E, 3ZA. A magistrate issues the warrant in their personal capacity and not as an officer of the court: at s 3CA. See also *Grollo v Palmer* (1995) 184 CLR 348. But they still discharge an important review function of the content and legitimacy of the warrant under the relevant legislation: *Smethurst v Commissioner of Police* (2020) 272 CLR 177. No doubt the Attorney-General and relevant Ministers will do a similar review for *IS Act* agencies, but they are not required to have the same legal training and experience as a magistrate.

92 *IS Act* (n 8) s 9; *ASIO Act* (n 8) ss 25, 25A, 26, 27, 27A, 27C.

from information sought from highly classified, well-placed human sources, or technically complicated electronic surveillance or interception methods – the disclosure of such capabilities might not only jeopardise ongoing security assessments or other intelligence activities but might compromise Australian strategic intelligence capabilities. In such a vacuum, the provisions of 'criminal intelligence' provisions have begun to fill the gap, which permit the court to examine the intelligence material (and potentially how it was obtained) but such material is not provided to the accused.[93] How then does an accused instruct a lawyer in their defence, when they cannot rebut evidence put in front of the court, or even know that such evidence exists? ACIC special investigations and operations (where undertaken for the purposes of intelligence gathering on federally relevant criminal activity) face similar challenges.[94]

B The Onshore/Offshore Distinction

One of the principal dangers represented by Australia's construction of the NIC is the delimiting of activities across the onshore/offshore dimension. In part, this reflects the pragmatism of conducting law enforcement and intelligence operations where technology has increasingly blurred geographic boundaries. But the observance of geographic limitations of power has important implications for national sovereignty and legislative competency. For example, law enforcement officers face difficulties enforcing Australian law outside Australia's territorial boundaries – the AFP cannot exercise policing powers outside Australia for crimes against Australian law without the assistance and cooperation of the host state.[95] This position differs for *IS Act* agencies and ASIO, who can (and indeed do) collect their intelligence and may undertake legally or morally questionable actions outside Australia that might offend another state's sovereignty.[96] In many cases, as the operations will not offend Australian law, a warrant is not required and therefore the Attorney-General will have no visibility of these activities.

A classified case study examined by the *Richardson Review* indicated ASIS displeasure at having to seek two independent Ministers' approval to undertake foreign intelligence collection, compared to security intelligence that ASIO or the AFP could gather with internal approvals.[97] The challenge here is that, although the AFP cannot exercise policing powers nor can ASIO exercise intelligence warrants outside Australia, both have an extraterritorial remit that permits them to gather

93 Brendan Walker-Munro, 'You Don't Need to Know: Australia's Experience with Criminal Intelligence as Evidence' (2021) 45(5) *Criminal Law Journal* 316, 325–6.

94 See, eg, *ACC Act* (n 8) ss 7C(2)–(4), 24A, 29A.

95 John McFarlane, 'The Thin Blue Line: The Strategic Role of the Australian Federal Police' (2007) 3(3) *Security Challenges* 91.

96 David Irvine, 'Freedom and Security: Maintaining the Balance' (2012) 33(2) *Adelaide Law Review* 295, 296, quoting Rodric Braithwaite, 'Defending British Spies: The Uses and Abuses of Intelligence' (2004) 60(1) *The World Today* 13, 13.

97 *Richardson Review* (n 2) vol 1, 220.

intelligence outside Australia.[98] That intelligence may inform the exercise of quasi-policing powers by ASIO[99] if that individual enters Australia.

Equally, the cooperative provision in section 13B of the *IS Act* permits some prevarication as to how *IS Act* agencies might collect intelligence in respect of offshore Australians, absent both a ministerial authorisation and an ASIO warrant. Section 13B enables ASIO to request ASIS to conduct activities that are outside Australia for producing intelligence on an Australian person or class of persons. Only those activities that ASIO could perform in Australia without a warrant may be undertaken (ie not intrusive methods of collection), but they do not require the issue of a ministerial authorisation under section 9.[100]

Ostensibly, this creates two potentially dangerous scenarios. The first is that section 13B notices allow ASIO to request ASIS to gather intelligence on an offshore Australian, without any external approval or oversight and by engaging in ASIS' core function – that function being the same as other equivalent agencies, committing espionage and breaking the laws of foreign states without being caught.[101] Though ASIO has discretion as to whether to issue the notice (and ASIS may not question their requirement to do so), ASIS retains discretion as to the actual activities undertaken. After all, espionage does not require a warrant.[102] The second is that ASIO may issue a section 13B notice for ASIS to produce intelligence on an Australian offshore in pursuit of offences touching on security and then share intelligence products with potential evidentiary value with NIC law enforcement agencies for the purpose of prosecuting those offences.[103]

In both scenarios, it is the purpose of the conduct engaged in which has created the greatest risk. Without giving thought to that underlying purpose (in this case, the purpose of the section 13B request), *IS Act* agencies may pollute or taint the information gathered. Though this might be the intended way those sections operate, it again creates the likelihood that an accused may face the admission of illegally procured evidence, in the sense that it was obtained by subterfuge and without consent of a foreign nation-state.[104] Of course, this is in the event that an accused is even permitted access to that evidence at all.

---

98 The *Richardson Review* recommended that ASIO be subject to the same authorisation process by the Attorney-General in circumstances where disclosure of intelligence gathered by ASIO might lead to the Australian person suffering death, serious injury, torture or other cruel, inhumane, or degrading punishment: ibid vol 2, 175.

99 For example, the arrest powers incidental to the questioning warrant regime: *ASIO Act* (n 8) pt III div 3.

100 *IS Act* (n 8) s 13B(5).

101 Roger D Scott, 'Territorially Intrusive Intelligence Collection and International Law' (1999) 46 *Air Force Law Review* 217, 219.

102 *IS Act* (n 8) s 13D.

103 Though the *IS Act* imposes strict secrecy principles on *IS Act* agencies, the *IS Act* also contemplates that intelligence that relates to 'serious crime' may be referred to the 'appropriate law enforcement authorities': ibid s 11(2)(c).

104 Section 138(1) of the *Evidence Act 1995* (Cth) permits a wide discretion to admit evidence that was obtained 'improperly' or 'in consequence of an impropriety', but this is interpreted broadly and usually against the evidence in question: *Ul-Haque* (n 35); *Parker v Comptroller-General of Customs* (2009) 83 ALJR 494; *Re Lim and Comcare (Compensation)* (2018) 78 AAR 253; *Kadir v The Queen* (2020) 267 CLR 109.

C The Collection/Assessment Divide

One of the other findings of the *Richardson Review* noted that NIC agencies should maintain a clear and strong distinction between collection agencies and assessment agencies. The *Richardson Review* noted that agencies are increasingly using open-source information (ie, information ordinarily available to the public, and is collected overtly and without resort to intrusive methodologies), but that the recent flood of open-source information – in particular from social media such as YouTube, Facebook and Twitter – the lines between collection and assessment was blurring unacceptably towards a fundamental change in the agency's nature, which the *Richardson Review* considered 'should not occur without clear articulation and a supporting legislative structure'.[105] So important is this principle that the *Richardson Review* recommended that the ONI ought to develop principles on open-source collection in conjunction with the relevant stakeholders (DIO, DoHA and IGIS) – though such principles would also assist in protecting privacy and ensuring good intelligence practice.[106]

Yet the lines between collection and assessment are practically non-existent in those NIC agencies that utilise criminal intelligence, namely the AFP, AUSTRAC, and ACIC.[107] Though ASIO undertakes collection and assessment functions under its overall function to combat threats to Australia's security,[108] it does so under a clear legislative ambit. That legislation provides for protections and safeguards for Australian citizens and residents in the form of warrants required for intrusive collection activities, and for reviews of adverse security assessments.[109]

None of the AFP, AUSTRAC, or ACIC require a warrant *specifically* to undertake intelligence collection activities on Australian citizens or permanent residents (unless the activity requires intrusion, such as telecommunications interception), nor are the findings of criminal intelligence practitioners open to any form of review.[110] Further, ACIC operates – as the *Richardson Review* identified[111] – under a 'hybrid' model whereby its warrant powers and interception capabilities may be deployed either for intelligence operations or special investigations authorised by the Australian Crime Commission Board.[112] Again, the intelligence

105 *Richardson Review* (n 2) vol 1, 251.

106 Ibid vol 1, 253.

107 All three NIC agencies are partners in the *ACIMS*, which mentions collection and assessment as critical parts of the Australian Criminal Intelligence Model: *ACIMS* (n 84) 3.

108 *Richardson Review* (n 2) vol 1, 245, 247. Both the *Hope Royal Commission* and the later Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies* (Report, July 2004) identified that separating collection and assessment activities for ASIO would unacceptably compromise ASIO's security functions: at vol 1, 245–7.

109 *ASIO Act* (n 8) pts III div 2, IV.

110 And, in fact, the legislation may specifically prohibit such review: *Administrative Decisions (Judicial Review) Act 1979* (Cth) sch 1; *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) ss 25, 38E. See also Walker-Munro (n 93) 319.

111 *Richardson Review* (n 2) vol 1, 271.

112 *ACC Act* (n 8) pt II div 2 ('examinations'), s 22 ('search warrants'). These powers may be utilised for collection or analysing intelligence or information on 'federally relevant criminal activity' while a special operation or investigation will involve federally relevant criminal activity: at s 4 (definition of 'federally relevant criminal activity').

outcomes of an ACIC intelligence operation are not subject to any form of review or public scrutiny.[113]

Further, some of the most intrusive capabilities available to NIC agencies unacceptably blur the lines between collection and assessment activities. Under recent amendments to the *Telecommunications Act 1997* (Cth), certain technical assistance may be compelled from telecommunications providers by the Director-General of Security[114] or the Attorney-General.[115] Both technical assistance notices and technical capability notices force providers to assist in, or build a capability for, the interception of certain communications passing over their networks. Whilst proportionality, feasibility, and costs criteria are provided for by that Act,[116] the threshold for approval is otherwise incredibly low. The notices need only require that the assistance or capability is required for 'the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory'[117] by either ASIO or an interception agency (which includes AFP and ACIC). The functions or powers also only need 'relate to' objectives which include, inter alia, both investigating offences and safeguarding national security.[118]

The *Richardson Review* did not recommend any changes to this mechanism of operation, recommending that this 'attribute-based' interception capability be retained in the new electronic surveillance legislation.[119] It is worth noting that the *Richardson Review* recommended retaining the overall coordination of intelligence products under the ONI,[120] as well as a principles-based scheme for sharing.[121] Yet in both cases, the *Richardson Review* recommended – despite the warnings of the IGIS – retention of the existing sharing provisions in addition to the updated provisions in the new electronic surveillance legislation. These would permit law enforcement agencies in the NIC to share information and evidence obtained under warrants or investigative methodologies with NIC intelligence agencies, and vice versa.[122]

To be clear, there remains nothing inherently wrong or unlawful about information sharing between law enforcement and intelligence agencies per se. Indeed, the *Richardson Review* found that a single information sharing Act would be likely to lead to less consistency, as 'much of the complexity in NIC information sharing legislation is a result of the distinct functions of NIC agencies and the different information with which they deal. This necessitates different information

113 Cf the recently expanded mandate of the Inspector-General of Intelligence and Security to oversee Australian Criminal Intelligence Commission investigations and operations: *Inspector-General of Intelligence and Security Act 1986* (Cth) s 8(3A).

114 *Telecommunications Act 1997* (Cth) s 317L (a technical assistance notice).

115 Ibid s 317T (a technical capability notice).

116 Ibid ss 317P, 317RA (for technical assistance notices), 317V, 317ZAA (for technical capability notices).

117 Ibid ss 317L(2)(c), 317T(2)(b).

118 Ibid ss 317L(2)(c), 317T(3).

119 *Richardson Review* (n 2) vol 2, 375–80.

120 Ibid vol 1, 332–41.

121 Ibid vol 2, 400–11.

122 Including, in particular, for the purposes of 'investigating or prosecuting of a criminal offence punishable by a maximum penalty of at least three years' imprisonment … crime-related proceedings, such as bail, parole, proceeds of crime, control order, preventative detention order or continuing detention order proceedings': ibid vol 2, 411.

sharing rules for each agency'.[123] Instead, the harm is likely to be inflicted when one seeks to pursue – whether accidentally or otherwise – the purpose of the other. ASIO and ASIS have no law enforcement function. The AFP are not in the business of conducting espionage. What the *Richardson Review* remained clear about is the fundamental thesis of Baker's paradigm: that spies are not cops, cops are not spies, and they should not try to take over one another's jobs. The *Richardson Review* also remained adamant that collection and analysis activities remain separated to preserve the agnosticism inherent in examining intelligence which an agency did not collect itself.

The current arrangements between the NIC intelligence agencies and law enforcement agencies, despite the *Richardson Review*'s optimism, do not strictly observe these separations and run counter to the findings of the earlier *Hope Royal Commissions* and intelligence reviews. Nor do the proposed principles of the new electronic surveillance legislation appear to adequately respect the divide between the roles of intelligence and law enforcement agencies. What in fact was required (and will be canvassed later) is a stringent requirement for information sharing that hinges on purpose – both the purpose for which the information was collected but also the purpose for which that information will be used by the agency it is given to. The thresholds for purpose will of course be different for each agency and is also contextual on the information gathered – but the absence of any strict provisions on purpose lead to potentially disastrous consequences if untested, unverified intelligence is used as evidence in criminal proceedings.

D Assumed Identities and Controlled Operations

Perfidy and manipulation are hallmarks of both espionage and serious crime, as those seeking to either undermine Australia's security interests or commit serious offending both wish to keep their activities away from the eyes of authorities. It is therefore axiomatic that both law enforcement and intelligence agencies will seek to utilise covert courses of action which may involve deceiving those potential offenders. Perhaps unsurprisingly, such broad powers are highly vulnerable to abuse and are thus subject to robust and tightly controlled legislative schemes for both assumed identities[124] and controlled operations.[125]

Under these legislative schemes, a controlled operation allows law enforcement or intelligence officers to plan for and execute an operation involving officers engaging in activity that prima facie constitutes an offence.[126] Under the *ASIO Act*, a similar legislative structure to controlled operations also permits the conduct of

123 Ibid vol 3, 47.

124 *Crimes Act 1914* (Cth) pt IAC. The *Richardson Review* recommended that the Defence Intelligence Organisation and DoHA remain excluded from the assumed identities scheme: *Richardson Review* (n 2) vol 1, 255.

125 *Crimes Act 1914* (Cth) pt IAB. Cf *Ridgeway v The Queen* (1995) 184 CLR 19.

126 *Crimes Act 1914* (Cth) ss 15GD, 15GF, 15GH, 15HA, 15HD.

special intelligence operations ('SIO').[127] Participants in SIO are immunised against criminal and civil liability in a similar manner to those in controlled operations.[128]

An assumed identity on the other hand permits an officer to apply to the chief officer of a law enforcement or intelligence agency to receive a new identity, including new identity documents (such as a passport or driver's licence) and immunity from any liability arising from the use of that identity in the course of official duties (as far as the use of the identity might be considered 'fraudulent' as it is not the officer's real identity).[129]

Yet when compared to controlled operations, an SIO requires ministerial-level approval by the Attorney-General and not officer-level approval by commissioner equivalent.[130] An SIO also requires a connection to one or more of ASIO's 'special intelligence functions'.[131]

Where these various legislative schemes contain the potential to cause issues arise on two fronts:

(a) First, the use of assumed identities by law enforcement agencies in circumstances where the use of that identity could be for an intelligence purpose, and vice versa for intelligence agencies using assumed identities for law enforcement purposes; and
(b) Secondly, the intersection of SIOs and controlled operations at the borders of counterespionage, politically motivated violence, foreign interference, and territorial border integrity[132] investigations.

As both law enforcement and intelligence agencies may apply to their own internal chief officers to obtain assumed identities,[133] and the factors determined by that chief officer before issuing an assumed identity are identical between NIC law enforcement and intelligence agencies,[134] an ASIO officer could ostensibly obtain an assumed identity for the purpose of 'investigation of, or intelligence gathering in relation to, criminal activity (whether a particular criminal activity or criminal activity generally)'.[135] Equally, an officer of a law enforcement agency like the AFP may obtain an assumed identity for the purpose of 'the exercise of

127 *ASIO Act* (n 8) pt III div 4.
128 Ibid s 35K; *Crimes Act 1914* (Cth) pt IAB div 3.
129 *Crimes Act 1914* (Cth) ss 15KB, 15KG, 15KJ, 15KK, div 4.
130 *ASIO Act* (n 8) s 35B(1). Cf *Crimes Act 1914* (Cth) s 15GF. Until the *Richardson Review*, such applications were also not reviewed by the senior lawyers of the Attorney-General's Department for accuracy and legislative compliance: *Richardson Review* (n 2) vol 2, 64.
131 Those being one or more of the functions under sections 17(1)(a), (b), (e) or (f) of the *ASIO Act*:
> (a) to obtain, correlate and evaluate intelligence relevant to security;
>
> (b) for purposes relevant to security, to communicate any such intelligence to such persons, and in such manner, as are appropriate to those purposes;
>
> …
>
> (e) to obtain within Australia foreign intelligence … and
>
> (f) to co-operate with and assist bodies referred to in section 19A in accordance with that section.

132 As both prima facie offences under the *Criminal Code* (n 8) and matters touching on 'security' under section 4 of the *ASIO Act* (n 8).
133 *Crimes Act 1914* (Cth) ss 15KA(1), (3).
134 Ibid s 15KB(2).
135 Ibid s 15KB(2)(a)(i).

powers and performance of functions of an intelligence agency'[136] like ASIO. The authorisations issued for assumed identities equally permit the use of those identities in a foreign country[137] – implicitly authorising offshore, non-intrusive intelligence collection in circumstances where that activity might fall outside the requirements in any of the NIC legislation.

Equally, there exists substantial opportunity for overlap to occur between SIOs and controlled operations in environments in which the law enforcement agencies of the NIC operate. AFP, ACIC or AUSTRAC investigations into criminality involving border integrity (such as smuggling or drugs), politically motivated violence, espionage, or foreign interference will permit controlled operations,[138] but may do so in circumstances where the investigation allows for the collection and analysis by law enforcement officers of intelligence relevant to security matters that are properly the jurisdiction of ASIO. ASIO may conduct an SIO into the same matters and end up obtaining evidence crucial to the prosecution of Commonwealth offences (but in circumstances where the collection of that evidence is not attended by the same safeguards and protections contemplated by the *Evidence Act 1995* (Cth)).

An SIO may also be grounds for the issue of an ASIO questioning warrant by the Attorney-General. This is because the test for connection required under the *ASIO Act* is merely that 'there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to an adult questioning matter',[139] a bar that is likely to be easily cleared if an SIO has already been authorised.[140] An identified person warrant, permitting the full range of ASIO covert collection powers, may also be granted if doing so would 'substantially assist the collection of intelligence relevant to security', language remarkably similar to the test required for an SIO authorisation.[141]

The final challenge confronting both assumed identities and SIOs is that ASIO is permitted to 'assist' law enforcement agencies with the performance of their functions.[142] Though this assistance provision is supposed to be subject to arrangements or directions issued by the Minister,[143] no such directions exist at the time of writing. The danger here is that an ASIO officer 'assisting' law enforcement may obtain an assumed identity for either intelligence or law enforcement purposes (or both) and then be included as a participant in a controlled operation. This would permit the circumvention of the ministerial approval of an SIO, as neither the application nor

136 Ibid s 15KB(2)(a)(ii).

137 Ibid s 15KB(5)(c). It requires only that the chief officer consider it 'reasonably necessary to do so': at s 15KB(6).

138 As either a 'serious Commonwealth offence' or a 'serious State offence that has a federal aspect': *Crimes Act 1914* (Cth) ss 15GE(2), (3).

139 *ASIO Act* (n 8) s 34BA(1)(b). An 'adult questioning matter' must relate to acts of espionage, politically motivated violence, or acts of foreign interference – all offences which the AFP might investigate: at s 34A.

140 As the requisite test for a special intelligence operation authority is the performance of a special intelligence function, which includes acts of espionage, politically motivated violence, or acts of foreign interference as matters touching on security: ibid ss 17(1)(a), 35C(2)(a).

141 Ibid s 27C(2)(b).

142 Ibid s 19A(1)(d).

143 Ibid s 19A(2)(a).

the approval process for controlled operations excludes the participation of ASIO officers per se.[144] Although lower risk, an AFP or ACIC officer could also be included as a participant in an SIO if named in an authorisation,[145] as the AFP has a function to provide 'police services' to intelligence agencies[146] and the ACIC can be authorised to conduct special investigations which may include ASIO.[147]

Though the *Richardson Review* confronted the differences between controlled operations and SIOs and concluded that no amendment of the SIO regime was necessary, this was from the perspective of limiting applications to the Director-General of Security and retaining authorisation for an SIO with the Attorney-General.[148] The *Richardson Review* also did not specifically consider SIOs and compare SIOs with controlled operations, nor did they consider the overlap with law enforcement agencies with respect to assumed identities.

Again, I suggest that the relevant test (which was not confronted by the *Richardson Review* per se) is one of purpose. It is entirely appropriate that law enforcement collect intelligence where it relates to a controlled operation, either to lead to other suspects or to identify new methods or means of offending. Equally, intelligence agencies obtaining evidence of criminal offending cannot be wilfully blind to the breaking of Australian law. Instead, both intelligence agencies and law enforcement should be satisfied (by recourse to the threshold set by legislation) that the boundaries of a controlled operation and/or SIO go only as far as – and no farther – than is required for the purpose of that operation.

E Conflicting Roles of Intelligence and Investigative Warrants

Historically, the term 'warrant' derives from English law, referring to a document to which a sovereign had affixed their sign-manual, a physical endorsement and indication of their pleasure with the contents of the document.[149] In many instances where the sovereign has intended that the sovereign's will be done through an intermediary or agent, they have issued a document expressing both the agent's appointment and the powers that agent is authorised to execute.[150] The term has retained these aspects throughout history: it remains a written authorisation of the power delegated from the sovereign, and a description of the power to be so executed by a named officer. In a general sense, warrants can authorise a wide variety of powers including searches, arrests, seizures of both evidence and goods, and the enforcement of judgments and liens.

---

144 An ASIO officer would be a 'civilian participant' and highly unlikely to be assigned any role of law enforcement as part of the controlled operation, but nonetheless permitted to utilise their intelligence collection and assessment skills under the imprimatur of the controlled operation authority: *Crimes Act 1914* (Cth) ss 15GC, 15GI(2)(h).

145 *ASIO Act* (n 8) section 35(1)(b) (definition of 'adverse security assessment') only requires that a 'person' be included in the authority.

146 *AFP Act* (n 8) s 8(1)(bf)(ii).

147 Even where such investigations are proactive rather than reactionary, and do not need to specify a particular offence or offender: *ACC Act* (n 8) s 7C(3).

148 *Richardson Review* (n 2) vol 2, 211–19.

149 William Reynell Anson, *Law and Custom of the Constitution* (Clarendon Press, 3rd ed, 1907) 50–1.

150 Ibid 59.

Within the NIC, warrants occupy a unique position as authorising certain activities within Australia that otherwise would be prima facie unlawful. Warrants obviously have no effect outside Australia, though they may have extraterritorial effect.[151] However, the outcomes associated with different classes of warrants may also have a wide range of effects, even though the initial purposes of those warrants may have been identical. For example, a stored communications warrant,[152] a computer access warrant,[153] and a surveillance device warrant[154] may all be sought either by law enforcement or intelligence agencies, and all have vastly different pre-requisites and approval mechanisms but all directed to the covert collection of private electronic information.

In addition, whilst the AFP is vested with significant arrest powers using reasonable force (both with and without warrants),[155] the ACIC has only limited powers of arrest,[156] and AUSTRAC has none. Neither ASIO nor any of the *IS Act* agencies have powers of arrest. However, ASIO could detain persons indirectly through the execution of a questioning warrant.[157] Under such warrants, ASIO also has the extraordinary power to regulate, control, silence, and even exclude legal representatives from questioning.[158]

It is a longstanding provision of law that interference with basic, fundamental rights may occur only with clear, unequivocal language.[159] Consistent with that interpretation, submissions to the *Richardson Review* expressed the view that any powers bearing similarity to arrest, questioning, or surveillance ought be attended by review by a judicial officer.[160] Yet, despite those submissions, the implementation of such a double lock system was rejected by the *Richardson Review*. In doing so, the *Richardson Review* observed that 'ASIO's questioning and detention warrants provide a single example of a form of double lock authorisation in Australia. ASIO's questioning and detention powers are extraordinary and "a measure of last resort"'.[161]

Those findings now warrant significant scepticism. A 10-year review of the questioning warrants regime in 2012 indicated that there was no empirical link between questioning warrants and terrorism prosecutions, raising the question

151 For example, a computer access warrant or data disruption warrant may permit access to a computer that is not located within the territorial boundaries of Australia, but the officer executing the warrant is (as the warrant thus protects the officer executing it from liability): *SDA* (n 8) ss 27A, 27KA.

152 *Telecommunications (Interception and Access) Act 1979* (Cth) pts 2-2 (for intelligence), 3-3 (for law enforcement).

153 *SDA* (n 8) s 27A (for law enforcement); *ASIO Act* (n 8) s 25A (for intelligence).

154 *SDA* (n 8) s 14 (for law enforcement); *ASIO Act* (n 8) s 26 (for intelligence).

155 *Crimes Act 1914* (Cth) ss 3W, 3ZA, 3ZC.

156 Pursuant to a arrest warrant of a witness who may be a flight risk: *ACC Act* (n 8) s 31.

157 *ASIO Act* (n 8) s 34C. The warrant may be for no longer than 28 days: at s 34BG(8).

158 See, eg, *ASIO Act* (n 8) ss 34FA, 34FB, 34FC, 34FF.

159 *Coco v The Queen* (1994) 179 CLR 427, 435–6 (Mason CJ, Brennan, Gaudron and McHugh JJ), 446 (Deane and Dawson JJ).

160 *Richardson Review* (n 2) vol 2, 56.

161 Ibid vol 2, 60.

of the purpose of retaining the warrant provisions.[162] At the time the *Richardson Review* was finalised in late 2019, ASIO questioning and detention warrants were indeed subject to judicial scrutiny.[163] The *Richardson Review* also had regard that the INSLM would finalise a review into those powers ahead of the sunset date of 7 September 2020. Yet despite that optimism, the INSLM did not finalise their review and on 10 December 2020 the Commonwealth Government passed legislation which repealed ASIO's detention power but retained and expanded the scope of questioning warrants.[164]

Other forms of warrant also blur the lines between intelligence collection and law enforcement: a dangerous position in situations where the very secrecy of such operations counters most persons' ability to understand their rights.[165] Search warrants for people, premises and vehicles may be obtained both under the *Crimes Act 1914* (Cth)[166] or the *ASIO Act*,[167] yet the former must be issued by a magistrate and the latter by the Attorney-General. Both warrants permit the same level of intrusion into a person's privacy and security yet are subject to vastly different approval processes (a magistrate acting *persona designata* versus an elected official). Similarly, the levels of interference with a person's privacy and dignity afforded by a surveillance device warrant obtained by police under the SDA[168] is the same as under the *ASIO Act*,[169] yet the former is issued by a judge or member of the Administrative Appeals Tribunal ('AAT'), and the latter authorised by the Attorney-General.

A third and final form of warrant also bears examining. Currently, the AFP can obtain a 'delayed notification search warrant' from a judge or nominated AAT member when investigating certain terrorism offences.[170] The name derives from the nature of the search – in contrast to normal search warrants, the delayed notification warrant authorises a search in the absence of the occupier or owner, who is notified after the fact but 'as soon as practicable' and within six months of the

162 Lisa Burton, Nicola McGarrity and George Williams, 'The Extraordinary Questioning and Detention Powers of the Australian Security Intelligence Organisation' (2012) 36(2) *Melbourne University Law Review* 415.

163 *ASIO Act* (n 8) s 34AB as repealed by *Australian Security Intelligence Organisation Amendment Act 2020* (Cth); Rebecca Welsh, 'A Judge in the Interrogation Room' (2010) *University of New South Wales Law Society Court of Conscience* 15, 15–16. See also Keiran Hardy and George Williams, 'Free Speech and Counter-Terrorism in Australia' in Ian Cram (ed), *Extremism, Free Speech and Counter-Terrorism Law and Policy* (Routledge, 2019) 172 <https://doi.org/10.4324/9780429469091>.

164 *Australian Security Intelligence Organisation Amendment Act 2020* (Cth).

165 It should also be noted that some warrants – such as network activity warrants – cannot yield evidence for use in criminal proceedings: *SDA* (n 8) ss 44, 45, 45B. However, the *SDA* also contains carve-out provisions allowing for evidence to be used in criminal proceedings: at ss 45(5), (7). Obviously, the *ASIO Act* contains no such provisions, and indeed permits the Director-General of Security to issue evidentiary certificates which must be accepted as prima facie statements of fact: *ASIO Act* (n 8) s 34AAC.

166 *Crimes Act 1914* (Cth) s 3E.

167 *ASIO Act* (n 8) s 25.

168 *SDA* (n 8) ss 14 (surveillance device warrant), 22 (retrieval warrant), 27A (computer access warrant), 27KA (data disruption warrant), 27KK (network activity warrant).

169 *ASIO Act* (n 8) s 26.

170 *Crimes Act 1914* (Cth) ss 3ZZBA(1), 3ZZBB(1), 3ZZBD(1), 3ZZBE(1)(i).

warrant being issued.[171] ASIO may also covertly search premises without notifying the owner or occupier under search warrants which, it is to be remembered, are authorised by the Attorney-General but remain in force for 90 days.[172]

If we recall that matters of security may include criminal offending, and many of the criminal offences pursued by the AFP may also touch on matters of security, the potential for abuse and unlawful interference with human rights from careless use of these warrants becomes unavoidable. Nowhere is this danger more amply demonstrated than in the NSW Supreme Court case of *R v Ul-Haque*.[173] Recorded admissions made by the accused were ruled inadmissible after ASIO officers detained him during a search warrant execution and subjected him to compulsive questioning.[174] At the time of the warrant there were also AFP officers present searching for evidence of potential terrorist offences (though the AFP were not present during the questioning). Adams J's obiter cautions against the conflation of the roles of law enforcement and intelligence collection:

> In my view, the conduct of ASIO … was well within the meaning of the phrase [oppressive]. In substance, they assumed unlawful powers of direction, control and detention. It was a gross interference by the agents of the state with the accused's legal rights as a citizen, rights which he still has whether he be suspected of criminal conduct or not and whether he is a Muslim or not.[175]

Adams J held the admissions were unlawful, having been obtained by oppressive conduct and that the ASIO officers in question had likely committed offences of assault and kidnapping, as well as the tort of false imprisonment.[176] This is perhaps the best example of the dangers of Baker's paradigm, and a stark reminder of the importance of remembering purpose in the exercise of such coercive powers.

Warrants are a substantial intrusion into the privacy, security, and safety of Australians, and offer substantial protection for officers who use them. Thankfully, the *Richardson Review* rejected submissions calling for the ACIC to be given covert search powers for the purpose of conducting intelligence operations.[177] Nor did the *Richardson Review* support the introduction of 'class based warrants' – that is, warrants authorising intrusions based on membership of a class of persons, rather than in relation to a specific named person.[178] The *Richardson Review* found such warrants were far too likely to infringe innocent persons in circumstances where no evidence was led to support the adoption of such broad sweeping powers.[179]

171 Ibid ss 3ZZDA, 3ZZDB, 3ZZDC.
172 *ASIO Act* (n 8) s 25(10).
173 *Ul-Haque* (n 35).
174 See ibid [34], [102], [121] (Adams J).
175 Ibid [95] .
176 Ibid [61].
177 *Richardson Review* (n 2) vol 3, 226–8.
178 Ibid vol 2, 118–19. Though a concession was made to allow for ministerial authorisations for *IS Act* agencies to target a class of terrorist organisations or when in support of military activities with the Australian Defence Force: at 123–7.
179 *Richardson Review* (n 2) vol 2, 114, 117.

F The Disruption of Cybercrime

The final aspect of Baker's paradigm that I intend to examine has arisen out of the evolution of cybercrime as a methodology of offending.[180] In many cases, the geographical distinctions related to onshore and offshore activities are at their most stretched, as computers and networks may be located in multiple sovereign states. In the cybercrime domain, ASD retains relative primacy for preventing, detecting, and disrupting cybercrime offshore, with ASIS providing an assisting role in respect of both collecting offshore intelligence activities and producing 'direct effects' against persons.[181] The *Richardson Review* confirmed the correctness of these offshore provisions being sited in *IS Act* agencies.[182]

Since the very early days of Federation, it has been lawful for the Commonwealth to use force to protect itself and its legal interests, and the military is a tool by which it may do so.[183] One purpose of ASD is to aid the ADF in support of military operations and to cooperate with the ADF on intelligence matters.[184] When supporting ADF operations, ASD's engagement is properly limited by legally permissible Rules of Engagement and only the Chief of Joint Operations (a senior military officer) may authorise ASD's engagement.[185] The purpose of ASD supporting military operations has been reinforced with the recommendation of the *Richardson Review* to provide limited criminal immunity to *IS Act* agencies and their officers in circumstances involving projection of cyber power in support of strategic objectives.[186] ASD is in all respects a strategic military capability – yet ASD has also concurrently been given a legislative direction to also prevent and disrupt offshore cybercrime, which is fundamentally the responsibility of law enforcement.[187]

Despite clear legislative guidance, the precise legal basis of Australia's cyber disruption powers is questionable under our international legal obligations. Whilst an in-depth analysis of those obligations is beyond the scope of this article, it is worth identifying our obligations as they expose some of the dangers inherent in the overlap between ASD and AFP powers. The *Charter of the United Nations*

180 Defined by the Australian Federal Police as both crimes committed against computers and networks, and crimes where computers are an integral part of the offending: 'Cyber Crime', *Australian Federal Police* (Web Page, 7 December 2021) <https://www.afp.gov.au/what-we-do/crime-types/cyber-crime>.

181 For Australian persons, a ministerial authorisation remains necessary: *IS Act* (n 8) ss 8(1)(ii) (activity that 'will, or is likely to, have a direct effect on an Australian person'), 9(1A)(a)(vii) (involving 'committing a serious crime by transmitting data or signals').

182 *Richardson Review* (n 2) vol 2, 171–7.

183 The Commonwealth Parliament has competence to legislate for 'the control of the forces to execute and maintain the laws of the Commonwealth': *Australian Constitution* s 51(vi). See also *R v Kidman* (1915) 20 CLR 425; *R v Sharkey* (1949) 79 CLR 121, 151 (Dixon J); *Australian Communist Party v Commonwealth* (1951) 83 CLR 1.

184 *IS Act* (n 8) s 7(1)(d).

185 Fergus Hanson and Tom Uren, 'Australia's Offensive Cyber Capability', *Australian Strategic Policy Institute* (Web Page, 2018) 6–8 <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2018-04/Australias%20offensive%20cyber%20capability.pdf?VersionId=ONFm43IrJWsYq2wBL7PlzJI7lbyuVIBO>.

186 *Richardson Review* (n 2) vol 1, 51, vol 2, 222–7.

187 *IS Act* (n 8) s 7(1)(c); *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018* (Cth). Cf Australian Federal Police, 'International Engagement: 2020 and Beyond' (Strategy, 2017) 15.

does not expressly prohibit states from engaging in reprisals or retorsions against illegal acts pre-emptively in certain circumstances or where the aggressors refuse to satisfy demands for redress.[188] Additionally, the *Convention on Cybercrime* ('*Cybercrime Convention*')[189] (the only international instrument with a specific focus on computer crime) permits states to impose jurisdiction over its nationals in accordance with domestic law.[190] However, both the *United Nations Charter* and the *Cybercrime Convention* make clear that the path to cybercrime responses is cooperative and diplomatic, not coercive or destructive. The *Cybercrime Convention* makes great reference to the use of mutual assistance requests for data, systems access, and disruption.[191]

As I have dealt with earlier, Australian law cannot take effect outside Australia's territorial boundaries – yet that is exactly what the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) achieves. It enables AFP and ACIC officers to apply for warrants to access computer data, adding/copying/deleting or altering that data, or intercepting information passing over a telecommunications network involving a target computer.[192] These warrants merely require the identification of a target computer or network, which need not be in Australia. As the warrant only has legal effect in Australia, it effectively immunises the officer or officers executing that warrant from any computer- or telecommunications-based offences they might commit in doing so. However, this does not spare them from the domestic laws of the foreign states applying to computers and networks on which they might intrude or disrupt. Neither the AFP nor the ACIC is required nor encouraged to inform any of ASIS, ASD, the Foreign Minister or the Department of Foreign Affairs and Trade ('DFAT') of its activities under computer access, network activity or data disruption warrants.

Therefore, the vesting of NIC agencies with such a remit as to encroach on the onshore/offshore and intelligence/law enforcement distinctions in cybercrime is not only domestically challenging but internationally risky. That anomaly was not explicitly confronted in the publicly available version of the *Richardson Review*. Permitting military capabilities to be used against Australians located offshore, even those engaging in criminal activity, also runs the risk of breaching Australia's international obligations under the *Geneva Conventions*[193] and may

188 Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, 902–5.

189 *Convention on Cybercrime*, opened for signature 23 November 2001, [2013] ATS 9 (entered into force 1 July 2004) preamble.

190 Ibid arts 22(1)(d), (4).

191 Ibid art 23. See also ch 3 s 2 (Title 1 – Mutual Assistance Regarding Provisional Measures), (Title 2 – Mutual Assistance Regarding Investigative Powers). Article 35 also requires states to establish a contact point for requests and advice known as the '24/7 Network'.

192 *SD Act* (n 8) pt 2 divs 4–6.

193 Requiring that military attacks be directed only against military objectives: *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978). See also Simon McKenzie and Eve Massingham, 'Taking Care Against the Computer: Precautions Against Military Operations on Digital Infrastructure' (2021) 12(1) *Journal of International Humanitarian Legal Studies* 224 <https://doi-org/10.1163/18781527-bja10036>.

also violate the host state's sovereignty, leading to diplomatic, economic or political repercussions.[194] Even the lowest level of cybernetic intervention by ASD could have international implications for Australia.[195] Unfortunately, the exact approval processes for law enforcement use of ASD capabilities have not been developed at the time of writing, leaving the question open as to exactly how and under what circumstances ASD's strategic capabilities are being used to disrupt cybercriminals.[196]

The use of strategic military assets to pursue criminal offenders and the vesting of disruptive powers with extraterritorial reach in law enforcement agencies with no oversight by the Foreign Minister or DFAT also raises serious questions. Adding to this mix, I can only observe that Australia has also recently passed Magnitsky laws with specific effect to curtail cybercrime.[197] Only time will tell how effective these reforms will be in imposing sanctions on offshore actors (whether state or non-state) who engage in such destructive behaviours against Australian interests.

III CONCLUSION AND RECOMMENDATIONS FOR REFORM

The *Richardson Review* was not shy in making recommendations to government, with 204 recommendations made in total. However, for the reasons I have explored above, there exists some scope for additional reform of the NIC legislation to better protect individual freedoms and human rights. Overarching these suggestions, the key term of 'purpose' is a common theme and one of incredible importance in ensuring our intelligence and law enforcement agencies act in a lawful way.

The first suggestion is that either the *IS Act* or *ASIO Act* be amended to make clear that intelligence gathered for ASIO by ASIS offshore pursuant to a section 13B notice must not be communicated outside ASIO (or at least not to a non-*IS Act* agency). Currently, an issue may arise where ASIO requests ASIS assistance under a section 13B notice, but the 'security' matter being considered by ASIO involves potential criminal conduct. ASIS must provide any intelligence on that conduct to ASIO as soon as practicable.[198] However, that intelligence may then be passed on to a law enforcement agency such as the AFP or ACIC,[199] blurring the lines between the permissible gathering of intelligence by a security agency and

194 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14, 107–8 [205].

195 Gary P Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 *American Journal of International Law Unbound* 207, 208–10 <https://doi.org/10.1017/aju.2017.57>.

196 It is also worth noting that the recommendations in the *Richardson Review* apparently relating to whether the foreign intelligence warrant legislation was 'fit for purpose' with respect to cybercrime has been redacted, leading to the question as to whether those provisions might be amended: *Richardson Review* (n 2) vol 3, 151–68.

197 The *Autonomous Sanctions Amendment (Magnitsky-Style and Other Thematic Sanctions) Act 2021* (Cth) inserted section 3(3)(c) into the *Autonomous Sanctions Act 2011* (Cth), allowing sanctions to be implemented for 'malicious cyber activity'.

198 *IS Act* (n 8) s 13F(2).

199 *ASIO Act* (n 8) s 18(3)(b)(i).

the impermissible gathering of evidence by lawfully questionable methods. An amendment to either Act that clarifies the operation of section 13B would ensure that such intelligence gathered by collection and analysis agencies is appropriately protected and only communicated for law enforcement or evidentiary purposes. Alternately, such information gathered under a section 13B request might be rendered inadmissible in criminal proceedings – leaving law enforcement able to use it for its own intelligence purposes without unnecessarily and arbitrarily infringing the rights of the person to whom that information relates.

The second possibility for reform involves minor clarification of the provisions relating to assumed identities in the *Crimes Act 1914* (Cth), which would have a substantive effect. Currently, the process of applying for an assumed identity appropriately recognises the distinction between applications by law enforcement versus those made by intelligence agencies.[200] However, that distinction is lost in the subsequent section of the Act dealing with the granting of assumed identities, which results in the anomaly that a law enforcement agency may grant an assumed identity for intelligence collection or an intelligence agency for the investigation of criminal activity.[201] The approval provision should enshrine in legislation the purpose under which any assumed identities are sought, granted, or modified.

A third suggestion would be to pass legislation ratifying the *Cybercrime Convention* as a law of Australia, like the approaches taken to Australia's other international obligations.[202] Though Australia has already created offences for the matters provided for in that Convention,[203] such an Act would make clear that Australia would prioritise international cooperation and use of mutual assistance requests over covert offensive cyber-capabilities in circumstances outside of armed conflict. The Act should also make minor amendments to the *Crimes Act 1914* (Cth), making clear that where NIC law enforcement agencies seek to use computer-based warrants against offshore targets (or targets where their location is unknown), they should notify either or both of the Foreign Minister or DFAT *prior* to the warrant being executed. Collectively, that legislation would provide statutory authority to the proposition that NIC agencies should only seek to use warrants which may infringe the sovereignty of a foreign state as an absolute last resort or in an emergency. Alternately, a provision similar to that previously required for operations and investigations by the Australian Crime Commission could establish a threshold test for such offensive cyber-capabilities to situations where 'traditional law enforcement methods are unlikely to be or have not been effective'.[204]

Fourthly, the new electronic surveillance legislation should clearly outline the purpose/s for which information may be intercepted by a law enforcement or intelligence agency. These purposes could be for the investigation of a serious,

200 *Crimes Act 1914* (Cth) ss 15KA(1), (3).
201 Ibid s 15KB(2).
202 For example, the *Geneva Conventions Act 1957* (Cth), the *International Criminal Court Act 2002* (Cth) and the *Australian Human Rights Commission Act 1986* (Cth), which ratify numerous person-based international instruments.
203 *Cybercrime Act 2001* (Cth).
204 Repealed by *Australian Crime Commission Amendment (Special Operations and Special Investigations) Act 2019* (Cth).

indictable or organised crime, as opposed to gathering intelligence on criminal or security matters. This would have the effect of then carving out the use of intelligence from criminal proceedings and circumvent any issues of secrecy as against the accused. In circumstances where a warrant proposes significant interference or obliteration of individual rights, the authorising officer (whether the Attorney-General or a judicial officer) must have in their mind the likely purpose/s for which any intercepted information will be used. This must – at the earliest possible stage – include a consideration of any potential criminal prosecution of a person arising from that material.

Of course, there may be situations where the gathering of intelligence is at such an early stage that it would not be possible or reasonable to expect the authorising officer to achieve a position on prosecution with any certainty. Also, under Australian law it remains the decision of the Director of Public Prosecutions whether a prosecution will proceed.[205] However, the new electronic surveillance legislation should adopt the findings of the *Richardson Review* and place the *purpose* of intelligence at the forefront of whether a warrant is authorised or not.[206]

Fifthly and finally, Parliament should amend the current oversight framework for the NIC. Though the *Richardson Review* found that the current oversight framework is effective, and these agencies possess a strong compliance culture,[207] there exists a significant and potentially harmful overlap in controlled operations and SIOs which has not been adequately addressed. Controlled operations and SIOs also have slightly different reporting obligations, with controlled operations only notified every six months to the Commonwealth Ombudsman and Minister for Home Affairs, whereas the IGIS must be notified when an SIO is approved and at least every six months thereafter.[208] Unfortunately, whilst the Ombudsman may disclose information to IGIS if it relates to an *IS Act* agency,[209] the IGIS has no equivalent provision to disclose information to the Ombudsman.[210]

Again, the findings of the *Richardson Review* note that the 'purpose' is the most important consideration for which a given action or activity is undertaken, particularly where that action or activity involves the abrogation of an individual's right to privacy, security or freedom.[211] This must be recognised in legislation which allows SIOs to be conducted into criminal offending, or controlled operations for the purposes of gathering intelligence. Therefore, Parliament should limit controlled operations in statute to be *only* for investigative or enforcement purposes, whilst SIOs be limited in statute *only* to intelligence collection or assessment. Alternately, the *ASIO Act* could be amended to provide that intelligence gathered under an SIO is not legally admissible in criminal proceedings against an individual.

---

205 *Director of Public Prosecutions Act 1983* (Cth) s 6.
206 *Richardson Review* (n 2) vol 1, 155.
207 Ibid vol 3, 256–7.
208 For controlled operations, see *Crimes Act 1914* (Cth) ss 15HM, 15HN. For SIOs, see *ASIO Act* (n 8) ss 35PA, 35Q.
209 *Ombudsman Act 1976* (Cth) s 35AB.
210 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34.
211 *Richardson Review* (n 2) vol 1, 155.

In terms of oversight, NIC law enforcement agencies must be required to notify either the Ombudsman or IGIS when a controlled operation is authorised (similar to the IGIS reporting required for SIOs) to ensure oversight of the approval and remove any doubt that a controlled operation is being done for an improper purpose. If the Ombudsman were determined as the oversight body, this would likely require an amendment allowing the IGIS to disclose information to the Ombudsman if it relates to the review of controlled operations, to ensure that *IS Act* agencies are not performing inappropriately as *agents provocateurs* of NIC law enforcement.

This article explains and confronts the spies-versus-cops paradigm, and how Australia's current NIC blurs the lines unacceptably in several key areas. However, nothing in this article should be taken as a criticism of either the *Richardson Review* or the agencies which they reviewed. The NIC is an immeasurably valuable strategic asset, populated by hard-working and noble officers seeking to protect Australia's national interests. The suggested areas of reform outlined above are more in the vein of improvements which will ensure that the NIC will continue to strike the right balance between protecting our human rights and legal obligations and keeping Australia and her citizens safe from cyphers and criminals.