2020

The perils of privacy and intelligence-sharing arrangements: The Australia–Israel case study

Daniel Baldino

Kate Grayson

This non-refereed article was originally published as:
Baldino, D., & Grayson, K. (2020). The perils of privacy and intelligence-sharing arrangements: The Australia–Israel case study. *Privacy Law Bulletin, 17* (7), 126-130.

This article first published in the *Privacy Law Bulletin.*

Baldino, D., & Grayson, K. (2020) The perils of privacy and intelligence-sharing arrangements: The Australia-Israel case study. *Privacy Law Bulletin*, *17*(7), 126-130.

Privacy Law
Bulletin

The perils of privacy and intelligence-sharing arrangements: the Australia–Israel case study

Dr Daniel Baldino** and **Kate Grayson

The aim of this analysis is to explore the governance frameworks and associated privacy and interrelated risks that stem from bilateral security arrangements such as the Australia–Israel intelligence relationship. In an era of expanding globalisation of intelligence, targeted oversight advances that are adaptive to global trends may serve to mitigate the potential costs and downsides of transnational intelligence exchange while respecting the privacy, rights and liberties of citizens and ensuring that sovereignty, human rights standards and rule of law remain protected.

Introduction

The Privacy Act 1988 (Cth) is the principal piece of Australian legislation for protecting the handling of personal information about individuals including the collection, use, storage and disclosure of personal information in both the federal public sector and in the private sector.[1] Whilst the Australian National Intelligence Community (NIC) agencies are subject to privacy requirements that are informed by the principles that underpin the Privacy Act, the Privacy Act itself does not cover all of the Australian intelligence and national security agencies.[2] These include the Australian Security Intelligence Organisation (ASIO) and the Australian Secret Intelligence Service (ASIS).

This matter is particularly pertinent given that spycraft is an international endeavour and remains an exceedingly secretive (and often misunderstood) arena. Certainly, Australia's bilateral intelligence liaisons with both traditional and non-traditional foreign counterparts have amplified post 9/11. But enhanced intelligence cooperation is not a cost-free exercise and can create diplomatic and political quandaries that expose a "darker side". Thus information-sharing advantages in a digital age will continue to co-exist with latent political pitfalls, accountability drawbacks and "security vs liberty" trade-offs. As such, Australian policymakers will need to carefully consider the effectiveness, liabilities and limitations of current global intelligence networks and associated political and institutional oversight mechanisms.

Indeed, it can be argued that the internationalisation of intelligence has spawned an "accountability deficit" that has been exposed, in part, by the restricted utility of informal agreements and off-the-record diplomatic arrangements. As such, this article will address and explore the privacy and related risks that stem from the Australia–Israel relationship as an example of how modern-day international security agencies cooperate in intelligence exchange. Such governance frameworks (and normative standards) remain primarily reinforced via memorandums of understanding (MOUs) and the constraints, or lack thereof, that are directed by two key accountability mechanisms — the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector-General of Intelligence and Security (IGIS).

Key takeaways

- Whilst the Australian intelligence agencies are subject to privacy requirements that are informed by the principles that underpin the Privacy Act, the Privacy Act does not cover Australia's intelligence and national security agencies.
- Australia, like many western liberal democracies, has a tendency to over-rely on the application of non-enforceable diplomatic assurances in sensitive security matters, which might incorporate a MOU as a subject-specific commitment between two parties. But such arrangements do not create or enforce legally binding obligations.
- Modern-day Israeli security linkages continue to exist alongside notable concerns surrounding a record of intelligence mismanagement and political maltreatment as well as a lack of appropriate domestic oversight safeguards to effectively govern the nature of such covert global intelligence enterprises.
- Australian policymakers need to carefully consider the effectiveness, liabilities and limitations of current global intelligence networks and associated political and institutional oversight frameworks.

- Australia's key oversight and accountability mechanisms remain constrained, deficient and legislatively restricted in the area of international intelligence cooperation.

Background

Australia and Israel formally established diplomatic relations in 1949 though there is no formal public acknowledgment of the origins of Australian–Israeli intelligence relationship. Nonetheless, in more recent years, the growing importance of defence and security collaboration has seen a deliberate attentiveness at a practical policy level. Moves towards enhancing mutual support in the defence and intelligence realm can be seen as picking up the pace due to factors like technological communications advancements as well as the political need to push back against threats like missile proliferation networks or transnational terrorism in a post-9/11 world.[3]

On the whole, international intelligence exchange remains integral to both strategic calculations and the operational work within intelligence services and connected government agencies. Various pieces of legislation, such as s 19 of the Australian Security Intelligence Organisation Act 1979 (Cth), do allow for cooperation with agencies and authorities of other countries approved by the relevant minister. As such, enhancing intelligence cooperation and respective surveillance systems — where appropriate and when in compliance with privacy laws and other regulations — should be seen as critical in helping to provide decision-makers with tactical and strategic warnings to better navigate global threat-based ecosystems.

Yet there are real and potential hazards as well as benefits in seeking such intelligence partnerships. In this context, "good relations" with Israel are not an end in themselves but should be seen as a means of securing Australia's national interests. Pointedly, a number of past security and intelligence controversies have served to spotlight the negative implications of excessive secrecy, the precariousness of international norms and the problematic status of non-binding and informal security protocols to direct preferred behaviour. Such past controversies have included the so-called passport affair in which Israel had counterfeited four Australian passports as part of an assassination plot as well as the circumstances surrounding the arrest and death of alleged agent of Mossad, Benjamin Zygier.[4]

Taken as a whole, any situation acting to forge and consolidate the conditions for the beneficial and constructive use of bilateral intelligence exchange should be underwritten by appropriate governance mechanisms, including oversight arrangements, which can provide suitable guidance and transparency to pilot the purpose, nature and limits of such intelligence activities and systems. Indeed, in past efforts to enhance collective intelligence capabilities with other countries, Hope J (who was most notably the appointed judge on a series of Royal Commissions on Intelligence and Security in Australia during the 1970s and 1980s) had observed:

> But there are risks, and costs. There is a danger that some of the information we are given access to will be deceptive or misleading. Operational co-operation may entail some loss of operational independence. Our agencies must beware of seeming to be in the pockets of their powerful counterparts. Of course, they must avoid being so. Australia's national interest does not and cannot exactly or entirely coincide with that of any other country, no matter how friendly.[5]

Memorandums of understanding

Australia, like many western liberal democracies, has a tendency to over-rely on the application of non-enforceable diplomatic assurances in sensitive security matters, which might incorporate a MOU as a subject-specific commitment between two parties (that will not create legally binding obligations). A MOU is usually used where it is considered preferable to avoid the stricter regulations and procedures of an official treaty.

Unlike treaties, these types of informal diplomatic agreements concerning the sharing of classified intelligence are typically kept confidential. Yet despite the fact that little is usually known about the precise details of these classified agreements, it had been revealed by former Secretary of the Department of Foreign Affairs and Trade (DFAT) Dennis Richardson that in 2006 a MOU had been entered into between an Australian and an Israeli intelligence agency about protocols for use of Australian passports.[6] Given few countries will divulge information on intelligence cooperation and its processes, this rare disclosure offered a distinctive window to examine the logic and methods used to govern such international exchanges and integrated safeguards.

Based on the Protective Security Policy Framework (PSPF), the Australian Attorney-General's Department recommends that informal arrangements regarding security classified information are documented for a limited time period and for an explicit purpose or activity.[7] At the same time, the risks and costs in the search for appropriate intelligence instructions and shared international practices will range from foreseeable to unpredictable. Despite some established rules such as the fact that the NIC is not permitted to share information branded AUSTEO (or Australian Eyes Only) with anyone who is not an Australian citizen, as captured by Richelson, "while some risks are common to virtually every intelligence cooperation arrangement, others may be more difficult to anticipate".[8]

Other related quandaries might involve circumstances where anticipated benefits are contradictory, free-riding behaviour, negative human rights implications like privacy breaches and the exposure to moral hazards. A moral hazard is a situation in which one party gets involved in a hazardous or precarious event knowing that it is protected against that risk and the other party will incur the cost. Further, it is worth noting that intelligence cooperation is fraught with polygonal problems and will continue to remain an intricate process when dealing with multiparty liaison links such as, for example, in dealing with the work of Mossad and its counterparts in Washington DC.

For instance, the US National Security Agency (NSA), in the dissemination of intelligence with Israel, has included information about Australian citizens without such sharing of information necessarily being consulted on or agreed to by Australian authorities. In 2013, another rare insight into the mishandling of the third-party rule was uncovered based on a leaked MOU by whistleblower Edward Snowden. Previously classified details had emerged of intelligence-sharing between the NSA and its Israeli counterpart, the Israeli Signals Intelligence National Unit (ISNU), on the sharing of signals intelligence. The MOU between the NSA and the ISNU had allowed NSA to share "raw SIGINT data" with Israel. Details showed the US Government handed over to Israel "raw" or "unevaluated and unminimised" signals intelligence including "transcripts, gists, facsimiles, telex, voice and Digital Network Intelligence metadata and content".[9]

On the other hand, the MOU between Israel and US had outlined:

> ISNU . . . recognizes that NSA has agreements with Australia, Canada, New Zealand, and the United Kingdom that require it to protect information associated with the UK persons, Australian persons, Canadian persons and New Zealand persons using procedures and safeguards similar to those applied for US persons. For this reason, in all uses of raw material provided by the NSA, ISNU agrees to apply the procedures outlined in this agreement to persons of the countries.[10]

So any mandate and protective features that were provided within the above provisions were directly undermined by the disclosure that Israel is also allowed to receive "raw SIGINT data" — information that has not been investigated and partitioned. Nor does it indicate if the Australian intelligence agencies or the other Five Eyes members mentioned had agreed or even been consulted about the nature of the MOU between the US and Israel. Typically, a receiving country is intuitively likely to promise not to share information onward to other countries without explicit permission; however, this is again not without risks in a world of mass digital surveillance and bulk interception. A major concern about the US sharing raw data with Israel is that there are no legally binding limits on the use of the data by the Israelis and that the information could even theoretically be shared with other partners that are not friendly towards, or inimical to, the interests of Australia.

In short, the leaked MOU draws attention to the flawed nature of such entity-to-entity level and less formal arrangements; arrangements that can act as an obstacle to accountability as well as pose conceivable dangers and blowback for Australian citizens' privacy and national interests.

Oversight and accountability mechanisms

So given the inherent risks and costs of foreign intelligence liaisons, such as the Australia–Israel intelligence relationship, robust legislative oversight mechanisms do remain a core component of how to best mitigate mistake, miscalculation or abuse given the rapidly changing cross-border information flow structures. Of course, intelligence agencies will need to maintain a degree of secrecy in both the collection and operation realms and therefore the standards of accountability and oversight will unavoidably differ from those applicable to other parts of government. At the same time, the public needs to have confidence that those intelligence agencies and their collaborative partners are acting with legality, proportionality and efficiency.

Parliamentary Joint Committee on Intelligence and Security

Parliamentarians bear a responsibility for both developing the legal and the institutional framework for oversight, and as the principal external overseers, for ensuring that oversight accomplishes the central targets of accountability and legitimacy. The PJCIS is constituted under s 28 of the Intelligence Services Act 2001 (Cth). However, the current piecemeal design of the PJCIS stands on highly contestable grounds as the best way of managing intelligence and security affairs that will increasingly incorporate the blurring of lines between domestic and foreign intelligence.

The PJCIS has a range of fundamental restrictions. Its oversight mandate is primarily limited to overseeing the administration and expenditure of NIC, addressing matters referred to it by the responsible minister or by a resolution of parliament, and reporting its recommendations to parliament and the responsible minister. So while the PJCIS might be powerful in the sense that it can examine the NIC's administration and expenditure, it also is in effect hamstrung, as it cannot review the intelligence-gathering and assessment priorities of the NIC nor does it have the power to initiate its own-motion inquiries into matters relating to the activities of

an NIC agency. This would entail bilateral intelligence and security sharing arrangements (with overseas partners like Israel).

In short, the functions of the PJCIS do not comprise the ability to cover particular operations that have been (or are being or are proposed to be) undertaken by the NIC. As captured by Labor MP Anthony Byrne in 2019:

> We need a committee that's more independent, a committee that does have remit into the operational activities of intelligence and security services and the capacity to initiate [its own] inquiries . . . it doesn't have the powers it needs to discharge [its] obligations on behalf of the Parliament and the Australian people.[11]

Alternatively, a legislatively strengthened remit of the PJCIS could be an important pathway of maintaining better oversight as well as in building a base for wider public confidence and assurance — especially given the new demands of operational responsiveness in the search for an even wider global network of security partners. As a starting point, there does appear to be considerable room for reform regarding the ambit, configuration and operation of the PJCIS.

Inspector-General of Intelligence and Security

Established by the Inspector-General of Intelligence and Security Act 1986 (Cth), the role and functions of the IGIS do remain a highly valuable component of the overall oversight infrastructure imposed on the NIC. In many ways, the Inspector-General's review and oversight of operational activities does supplement approaches and attitudes within the PJCIS.

The IGIS is an independent executive oversight body whose legislative task does enable it to provide assurances that the NIC is acting with legality, propriety, under ministerial direction and with consistency in regard to human rights standards. The IGIS has significant powers, akin to those of a Royal Commission, which can include the ability to review information and require persons to answer questions and produce documents. It can also investigate complaints and undertake regular inspections of agency files and documentation to identify potential problems with compliance and control frameworks within agencies.

However, what is less apparent is whether the IGIS has the ability or the resources to oversee international intelligence-sharing agreements, like those between Australia and Israel. In fact, there are very few mechanisms at either national or international levels that have the ability to deal with and regulate the intricate or multilayered cross-jurisdictional aspects of intelligence cooperation in any detail.

The main role of IGIS is to oversee the activities of the intelligence agencies as opposed to why they should be conducting these activities. This is an important distinction. At the same time, extending the remit and resourcing of the IGIS commensurate to match with the scale and complexity of the entire NIC would help to support its oversight objectives related to issues of legality and propriety. And other current human rights and related debate points associated to the extended powers of the NIC — including access to, and sharing of, citizen data — are likely to only intensify the workload for the IGIS.

Conclusion

The formation of intelligence agreements such as the Australia–Israel should always be predicated on the careful assessment and management of the risks, including privacy, associated with it. Any situation of fashioning executive agreements to underpin intelligence coalitions should be underwritten by a plurality of appropriate governance mechanisms, including strong institutional and legislative oversight arrangements which can provide guidance and transparency to ensure compliance and quality control. Legislative oversight bodies should be equipped to support the integrity and reputation of intelligence processes as well as investigate allegations of wrongdoing linked to international intelligence cooperation.

The use of diplomatic assurances is principally based on a notion of trust that the receiving state will uphold particular moral obligations and standards of behaviour. However, the practices of informal agreements, while proving some level of behavioural check, have proven to be highly fragile and can be undoubtedly circumvented. In this sense, robust formal oversight systems and the advance of legally constrained intelligence parties that are shaped towards respecting personal information and human rights could help to counter human rights and related concerns while assisting to avert future political flash points and diplomatic clashes.

The effective oversight of the intelligence agencies will require a strengthening of the PJCIS' legislative powers to widen its remit to include an ability to consider and investigate operations matters as well as conduct its own independent inquiries. Further, the IGIS, an independent statutory officeholder, should be allowed to oversee intelligence matters that might extend to involve other government departments, such as DFAT.

The sharing of information is ultimately a balance of interests. Australian citizens should expect that the actions of their intelligence and security agencies are properly scrutinised and held to account while items like privacy, rights and liberties, and rule of law do remain fundamental democratic and legal principles.

Dr Daniel Baldino
Associate Professor
Discipline Head of the Politics and International Relations Program, School of Arts and Sciences
University of Notre Dame, Fremantle
daniel.baldino@nd.edu.au
www.notredame.edu.au

Kate Grayson
Independent researcher
Previously served as an adviser to the late former senator Russell Trood
kategrayson@hotmail.com

Footnotes

1. Australian Government Attorney-General's Department, Privacy, accessed 14 September 2020, www.ag.gov.au/rights-and-protections/privacy.
2. See Office of the Australian Information Commissioner, Government agencies, accessed 17 September 2020, www.oaic.gov.au/privacy/your-privacy-rights/government-agencies/.
3. S Morrison "Address to the Sydney Institute" (speech, Sydney, 15 December 2018) www.pm.gov.au/media/address-sydney-institute.
4. For full case studies, see: D Baldino and K Grayson "The Australia–Israel security relationship, oversight and the paradox of intelligence sharing" (2020) 74(5) *Australian Journal of International Affairs* 578.
5. *Royal Commission on Intelligence and Security Third Report [re Intelligence Co-Ordination Machinery] (Copy No 24 — Commission Working Copy)* NAA: A8908, 3A (1976) 147.
6. Cth Official Committee Hansard, Senate Foreign Affairs, Defence and Trade Legislation Committee, Budget Estimates, 2 June 2010.
7. See Attorney General's Department (Cth), Protective Security Policy Framework, Australian Government Protective Security Policy, accessed 20 September 2020, www.protectivesecurity.gov.au/about/Pages/default.aspx.
8. J T Richelson "The Calculus of Intelligence Cooperation" (1990) 4(3) *International Journal of Intelligence and CounterIntelligence* 307 at 315.
9. G Greenwald, L Poitras and E MacAskill "NSA shares raw intelligence including Americans' data with Israel" *The Guardian* 12 September 2013 www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.
10. US–Israeli Memorandum of Understanding (undated), accessed 23 September 2020, https://edwardsnowden.com/2013/09/11/us-israeli-memorandum-of-understanding/.
11. Quoted in J Norman "MP calls for parliament's powerful intelligence committee to have greater oversight of security agencies" *ABC News* 12 June 2019 www.abc.net.au/news/2019-06-12/labor-wants-more-power-for-parliamentary-intelligence-security/11203166.