COMMONWEALTH OMBUDSMAN

Submission by the Commonwealth Ombudsman

Response to Elect

Reform of Australia's electronic surveillance framework discussion paper

Submission by the Acting Commonwealth Ombudsman, Penny McKay

February 2022

Introduction

In December 2021, the Government released the Reform of Australia's electronic surveillance framework discussion paper (the discussion paper). The discussion paper covers a wide range of electronic surveillance issues and provides an overview of how the Government proposes to reform Australia's electronic surveillance legislative framework. The proposed reforms stem from, but are not limited to, recommendations of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Comprehensive Review).

The purpose of the Office of the Commonwealth Ombudsman (the Office) is to:

- provide assurance that the agencies we oversee act with integrity and treat people fairly, and
- influence systemic improvement in public administration.

Since the early 1990s the Office has provided assurance that Commonwealth, State and Territory law enforcement, integrity and regulatory agencies comply with statutory requirements and have sound administrative practices in relation to the use of certain covert, intrusive and coercive powers. Our role has expanded over time and we now oversee the use of powers by 21 agencies across 13 legislative regimes.[1]

Question 31 of the discussion paper poses the question:

> *What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?*

Electronic surveillance reform is an opportunity to enhance the assurance the Office provides to Parliament and the Australian community, by strengthening and streamlining our oversight framework.

The current framework for our oversight of agencies' use of covert, intrusive and coercive powers (including electronic surveillance) is scattered across various Acts. The legislative provisions governing our oversight are inconsistent across different regimes, and generally focus on strict legislative compliance by agencies with less or no regard to broader issues of propriety or proportionality. The current framework makes it difficult for the Office to:

- prioritise issues and practices that pose the greatest substantive risk
- investigate and report on issues that cut across different regimes and agencies
- consider proportionality and best practice in agency decision-making when using covert and intrusive powers, and
- support agencies to identify and address the root cause of non-compliance and manage risks across regimes.

Electronic surveillance reform is an opportunity to re-set the oversight framework to allow our Office to deliver stronger, risk-based oversight of agencies' use of covert, intrusive and coercive powers.

This submission outlines:

- how the Office currently oversees law enforcement activities
- limitations in the current framework of Commonwealth Ombudsman oversight, including

[1] We also have a review function under Part V of the *Australian Federal Police Act 1979* and, in the Office's capacity as the ACT Ombudsman, oversee agencies' compliance with certain covert and intrusive powers under ACT legislation.

the disparate nature of oversight provisions which leads to fragmentation and inefficiencies, and
- options for reform building upon the recommendations of the Comprehensive Review, proposing 9 features of an effective oversight framework for the Commonwealth Ombudsman.

We welcome the opportunity to contribute our thinking on reform to electronic surveillance legislation and remain keenly interested in the views of stakeholders as this reform progresses.

Background

How does the Commonwealth Ombudsman currently oversee law enforcement activities?

As noted by the Comprehensive Review, electronic surveillance activities are inherently covert and highly intrusive. This means an individual generally does not know when they are the subject of these activities and, as such, has less opportunity to challenge an agency's use of electronic surveillance powers.[2]

The Office currently oversees the use of electronic surveillance powers by 21 law enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Surveillances Devices Act 2004* (SD Act).[3] These include use and access to telecommunications data, telecommunications interception, stored communications, surveillance devices, tracking devices, computer access warrants and recently passed powers like data disruption warrants and international production orders.

The oversight role we perform varies across legislation, depending on the power being inspected. For example, our oversight of telecommunications interception under the TIA Act is of Commonwealth law enforcement agencies' compliance with record-keeping and destruction obligations. Unlike other regimes under the TIA Act, we do not inspect State and Territory compliance with Commonwealth telecommunications interception powers, and our ability to provide assurance on matters beyond record-keeping and destruction obligations is limited.

The Office is also responsible for overseeing the use of non-electronic surveillance – but still intrusive, and in some cases covert – law enforcement powers. This includes powers under the *Crimes Act 1914* (Crimes Act) (controlled operations, delayed notification search warrants, powers to monitor extended supervision orders, and account takeover warrants) and industry assistance powers under Part 15 of the *Telecommunications Act 1997* (Telecommunications Act). These powers are often used by agencies alongside electronic surveillance powers.

Further, the Office is responsible for overseeing the use of compulsory examination powers by the Fair Work Ombudsman and the Australian Building and Construction Commission, and the administration of complaints against Australian Federal Police (AFP) members under Part V of the *Australian Federal Police Act 1979* (the AFP Act).

Our factsheet on the oversight of the use of covert, intrusive and coercive powers, which is available on our website, further outlines these functions.[4] A diagram of the overarching

[2] Comprehensive Review, Volume 2 at 31.1 to 31.3.
[3] This includes our oversight of the Attorney-General's Department's activities as Australian Designated Authority for international production orders under Schedule 1 of the TIA Act. See Attachment A for the Commonwealth oversight of National Intelligence Community agencies.
[4] Commonwealth Ombudsman, Oversight of the use of covert, intrusive and coercive powers, Oversight of the use of covert, intrusive and coercive powers (ombudsman.gov.au).

Commonwealth oversight of national intelligence community agencies is at **Attachment A**.

Inspections

To the extent permitted by differences in legislative provisions across regimes, the Office aims to take a consistent approach to overseeing these powers. We:

- conduct inspections of agency records (policies and procedures as well as records of individual warrants, authorisations, and activities)
- discuss the use of powers with agency officers and personnel, and
- work with agencies and departments that administer the legislation (most often the Department of Home Affairs) to address emerging issues or issues cutting across different regimes and/or different agencies, such as the emergence and use of new technologies by targets or agencies.

We make findings based on our inspections, which we provide to agencies in post-inspection reports. Some of these findings result in the Office making recommendations or suggestions to agencies about how they can or should address non-compliance, or take action to mitigate the risk of future non-compliance.[5] Our aim is for these recommendations and suggestions to be achievable and clear, to enable meaningful improvements to agency compliance. Key findings from our inspections are also provided in reports to the relevant Minister (who tables those reports in Parliament), or in some cases directly to Parliament (through the Office tabling the report), providing transparency and assurance to Parliament and the Australian community.

The frequency of our inspections and reporting differs across regimes, depending on the relevant legislative provisions and the volume of agency use of the powers.

As noted in the discussion paper,[6] State and Territory bodies currently oversee State and Territory agencies':

- use of interception powers under the TIA Act
- use of surveillance device powers under state and territory legislation, and
- activities more broadly.

Other relevant functions of the Commonwealth Ombudsman

Under the *Ombudsman Act 1976* (the Ombudsman Act),[7] the Commonwealth Ombudsman has the power to conduct an own motion investigation into action that relates to a matter of administration by a department or a prescribed authority. We recently used these powers to investigate the AFP's use and administration of telecommunications data powers from 2010 to 2020, in particular access to and use of location-based services, colloquially known as 'pings'. The investigation report was published in April 2021.[8]

We made 8 recommendations to assist the AFP in addressing these issues and implementing processes to prevent their recurrence. This kind of in-depth investigation across multiple reporting periods cannot be achieved through the Ombudsman's routine inspections under the

[5] Commonwealth Ombudsman, Understanding inspection reports fact sheet, Understanding inspection reports (ombudsman.gov.au).
[6] Reform of Australia's electronic surveillance framework discussion paper, Part 5: Safeguards and Oversight, pg. 64.
[7] Sections 5(b) and 8 of the *Ombudsman Act 1976*.
[8] Commonwealth Ombudsman, Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020, Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020 (ombudsman.gov.au).

TIA Act, and is limited to Commonwealth agencies within our jurisdiction.

The Commonwealth Ombudsman also has the power to investigate complaints about the use of electronic surveillance powers by Commonwealth agencies. However:

- this relies on an individual knowing these powers were used to make a complaint, and
- we do not have jurisdiction over complaints regarding State or Territory agencies' use of Commonwealth electronic surveillance powers.

Submission

Limitations in the current framework for Commonwealth Ombudsman oversight

As discussed above, the Office's current remit for electronic oversight varies depending on the power or regime – in some regimes our oversight is substantially narrower (for example, in relation to telecommunications interception) than in other regimes. In principle, there is no reason why this should be the case. The Comprehensive Review concluded that '[t]he reason for this discrepancy appears to be purely historical'.[9] There are also significant discrepancies across regimes in relation to the frequency of inspections and frequency and tabling arrangements for reports.

The current framework embeds fragmentation and inefficiency in oversight. The specific and disparate nature of oversight provisions makes it difficult for us to:

- prioritise systemic or otherwise significant issues as they arise across regimes and/or across agencies
- shift our time and resources away from compliance issues which have a minor or negligible impact, and
- help agencies identify and mitigate significant risks relating to issues that potentially result in non-compliance.

Increasingly, we see agencies conducting large operations using a range of covert and intrusive powers (not limited to electronic surveillance powers). Often, the use of these powers in such operations also spans multiple agencies in joint operations. The current inconsistencies in oversight provisions result in a narrow and siloed approach where we inspect and report on agencies' use of different powers separately. This creates difficulties in providing strong assurance to Parliament and the Australian community, as we are generally not able to consider the full operational context in which those powers are being used.

As previously noted, the Commonwealth Ombudsman's own motion investigation powers do not apply to State and Territory agencies, including those using Commonwealth electronic surveillance powers. This limits our scope to investigate issues and risks across regimes and agencies.

Options for reform

Electronic surveillance reform presents an opportunity to reframe Commonwealth Ombudsman oversight of the use of electronic surveillance powers, and other covert and intrusive powers, by agencies. It is an opportunity to consider how we can most effectively add value to the agencies we oversee, and to provide assurance to the Parliament and the Australian community on how those agencies use covert and intrusive powers.

[9] Comprehensive Review, Volume 2 at 31.19.

Findings of the Comprehensive Review

The Comprehensive Review observed that 'the [Inspector-General of Intelligence and Security] and Commonwealth Ombudsman are independent and have access to strong powers.'[10]
The Review also made recommendations aimed at strengthening this oversight system, including that oversight should:

- take a functional approach, with flexibility to deliver substantive oversight when and where required, including as agencies' activities, functions or powers evolve
- be comprehensive and robust, with no matters off-limits and flexibility to focus on areas of potential risk,[11] and
- be centralised and consistent, with the Office having oversight responsibility for the use of Commonwealth electronic surveillance powers by all agencies other than ASIO, including State and Territory agencies.[12]

Recent findings of the Parliamentary Joint Committee on Intelligence Security (PJCIS)

In its review of the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, the PJCIS proposed the Office should be able to take a propriety approach to oversight.[13] This would be similar to the framework for oversight of intelligence agencies by the Inspector-General of Intelligence and Security (IGIS). As noted by the Comprehensive Review,[14] the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) provides the IGIS with:

- comprehensive oversight of the legality and propriety of agency activities and their conformity with human rights
- considerable flexibility to determine how to allocate oversight resources and efforts, and
- strong powers to obtain information from agencies and people working with agencies.

Is the IGIS oversight framework suitable for the Commonwealth Ombudsman?

While an oversight framework for the Office may share similarities with the oversight framework applied by the IGIS, it may not be appropriate or effective for an amended Ombudsman oversight framework to replicate the current IGIS framework in all respects. There will continue to be key differences in the operating and oversight environment, as between the Ombudsman and the IGIS. For example:

- The IGIS currently oversees all functions of the agencies in its jurisdiction (with a limited exception for ACIC and AFP network activity warrants introduced by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (SLAID Act)). Law enforcement agencies at the Commonwealth, State and Territory level will continue to be subject to oversight across their full range of functions not only by the Commonwealth Ombudsman, but also other bodies such as ACLEI, and State and Territory oversight agencies.

- A significant proportion of law enforcement agency activities will continue to be directed towards the gathering of evidence. Material brought into evidence is tested – and subject to challenge – through judicial processes. This is not the case for the activities of agencies

[10] Comprehensive Review, Volume 1 at 3.115.
[11] Comprehensive Review, Volume 2, page 435.
[12] Comprehensive Review, Volume 2, pages 432-435, page 435, and Recommendations 129 and 131.
[13] PJCIS Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020, August 2021, page 126, paragraph 6.34.
[14] Comprehensive Review, Volume 2 at 31.9.

within the oversight jurisdiction of the IGIS.

- Commonwealth, State and Territory human rights commissions have jurisdiction over human rights issues arising in law enforcement agencies – whereas the Australian Human Rights Commission does not have jurisdiction over agencies overseen by the IGIS.

Our focus is on a model for Commonwealth Ombudsman oversight which will provide greatest assurance in the law enforcement context. It will be important for the new electronic surveillance legislation to have strong information sharing provisions, and to ensure our Office can engage appropriately with IGIS and other Commonwealth, State and Territory bodies on matters of oversight.

Legislative drafting options

At the drafting stage, it will be important to ensure clarity and consistency in provisions governing oversight by the Office. Currently, the provisions governing our oversight are spread across the TIA Act and SD Act and, for powers beyond electronic surveillance, in a range of legislation including the Telecommunications Act, Crimes Act and AFP Act.

One option would be for our oversight provisions to sit in the Ombudsman Act itself, like the way the IGIS's oversight powers currently sit in the IGIS Act. Benefits could include:

- Less risk of incremental fracturing across assurance oversight functions whenever electronic surveillance or other coercive powers are amended or introduced for law enforcement. It would be easier to maintain a consistent, flexible and effective risk-based approach to oversight across regimes and agencies.

- Our oversight provisions would sit centrally in legislation administered by the Attorney-General (the Ombudsman Act), consistent with the Attorney-General's responsibility for oversight matters. Currently our oversight provisions are spread across legislation administered by the Minister for Home Affairs, Minister for Communications and Minister for Industrial Relations (currently the Attorney-General) for our ABCC and FWO oversight.

At this stage of the reforms, our Office is not wedded to a particular oversight framework. We will work with the Electronic Surveillance Reform Taskforce to consider the ideas and views of stakeholders, including those put forward in response to the discussion paper.

Features of a framework for effective oversight by the Commonwealth Ombudsman

We support the proposal for our Office to oversee Commonwealth, State and Territory law enforcement agencies' use of electronic surveillance powers. We also support the functional approach to oversight outlined by the Comprehensive Review and agree there should be flexibility for our Office to focus on areas of potential risk, with no matters off-limits.

This would enable us to take a more holistic approach to oversight while also providing the flexibility to focus on the areas of greatest risk, including where those risks cross different regimes and/or arise across different agencies. The ability for our Office to conduct investigations into issues that cut across different regimes and/or different agencies – building on our current own motion investigations role and expertise – would also contribute to this holistic approach.

As discussed above, the Office currently oversees law enforcement's use of electronic surveillance powers and a broader range of covert and coercive powers. In principle and in practice, law enforcement covert, intrusive and coercive powers should be subject to a

consistent, robust and coordinated oversight framework. To the extent changes are made so the Office is better placed to deliver comprehensive, flexible and risk-based oversight of law enforcement electronic surveillance powers, this same model should apply to equivalent law enforcement powers such as controlled operations[15] and industry assistance.[16]

In our view, an effective framework for Commonwealth Ombudsman oversight has the following features:

1. **Compliance** – We support the Office being responsible for comprehensive oversight of the compliance of law enforcement agencies' use of coercive and covert powers – including, but not limited to, electronic surveillance powers.

2. **Proportionality** – We seek a clear legislative basis to enable the Office to consider the proportional of use of powers and best practice that sit outside strict legal compliance.

3. **Risk-based** – We seek the flexibility to take a risk-based approach to our oversight role, including determining what matters we focus on with no matters off-limits, and how and when we conduct inspections.

4. **Consistency** – We seek an oversight model that applies consistently across the range of covert, intrusive and coercive powers we oversee (not limited to powers in the TIA Act and SD Act).

5. **Investigations** – We support a legislative basis for our Office to conduct own motion investigations into issues cutting across different regimes and/or different agencies including at State/Territory level.

6. **Access and record keeping** – We should continue to have independent access to agency information, premises and officers to support our oversight. Agencies will need to keep sufficient records to demonstrate compliance.

7. **Continuous improvement –** We should have a strong footing to support agencies' continuous improvement by sharing expertise on best practice and regularly reviewing agencies' guidance materials.[17]

8. **Information sharing –** We should have strong information sharing provisions with other Commonwealth, State and Territory oversight and regulatory bodies, supported by clear legislation, to ensure oversight issues are dealt with comprehensively.

9. **Reporting** – We support Ombudsman reports being tabled in Parliament in full[18] and publishing unclassified reports how and when we deem necessary.[19]

---

[15] Under Part IAB of the *Crimes Act 1914.*

[16] Under Part 15 of the *Telecommunications Act 1997.*

[17] Comprehensive Review, Volume 3 at 40.138 and Recommendation 171.

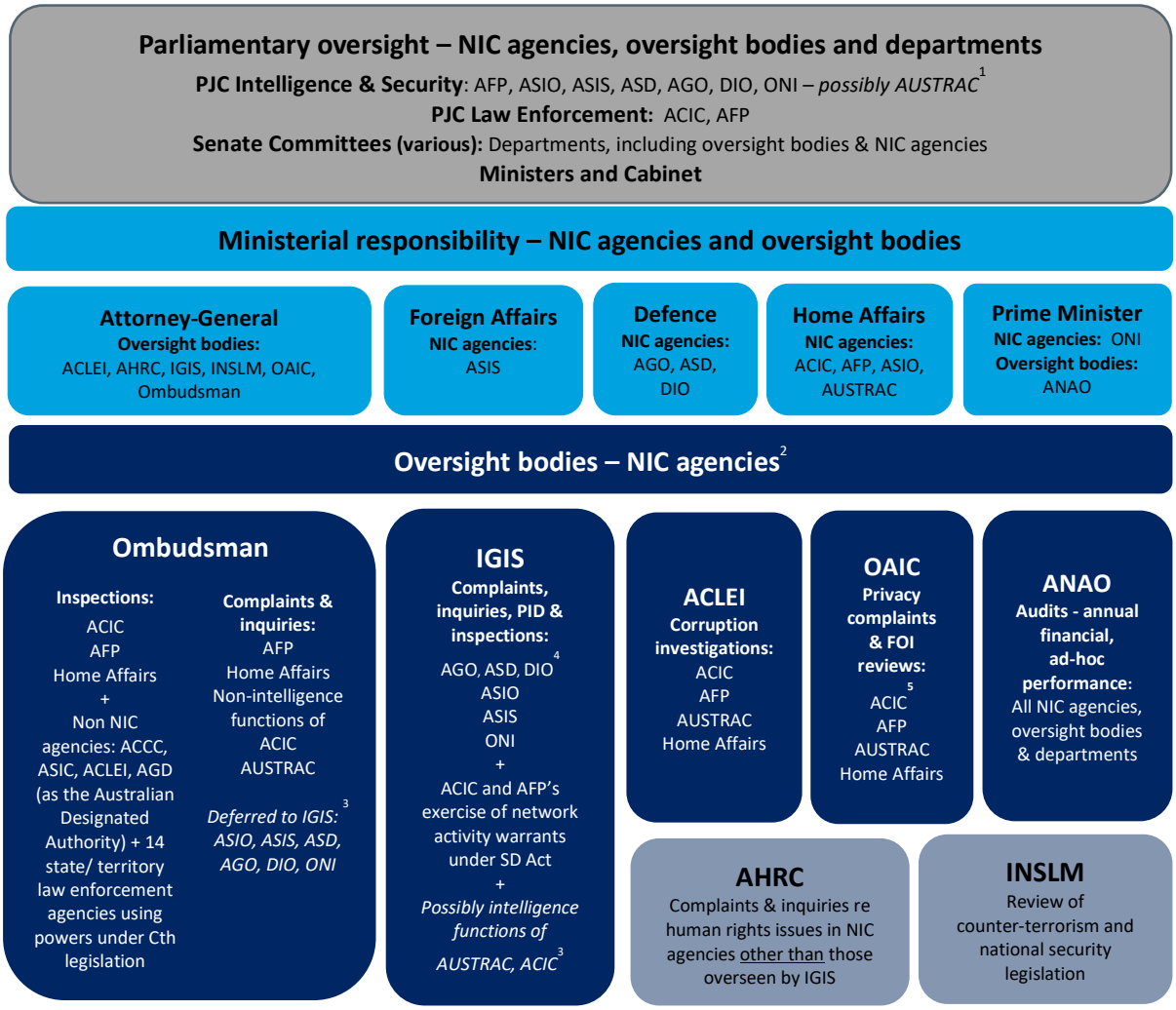
[18] Comprehensive Review, recommendation 132 – Ombudsman reports should be tabled by the Minister in full, except where information has been redacted to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations, the privacy of individuals or to avoid danger to a persons' safety. In practice the Office works with agencies to ensure this information is not included in reports in the first place, so redactions have not been required.

[19] Comprehensive Review, Volume 3 at 40.131 to 40.133.

A framework with these features would provide greater flexibility for our Office to prioritise systemic or otherwise significant issues as they arise. Legislation that provides this type of flexibility should also set out clear expectations for meaningful oversight of agencies' powers. The legislation governing our oversight should ideally strike a balance between providing discretion in how we manage our oversight functions while providing clarity about our oversight role.

As acknowledged by the Comprehensive Review and the PJCIS, effective oversight by this Office also relies on sufficient resourcing. We will work with relevant agencies to ensure our resourcing needs are considered in the development and implementation of the new electronic surveillance framework.

Attachment A: Commonwealth oversight of National Intelligence Community agencies



1. The Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (reviewed by PJCIS) seeks to extend IGIS oversight over AUSTRAC and ACIC intelligence functions, and PJCIS oversight over AUSTRAC intelligence functions
2. The courts and the AAT also review some decisions of NIC agencies. The Independent Reviewer of Adverse Security Assessments reviews some ASIO adverse security assessments.
3. Although the Ombudsman formally has jurisdiction over these agencies, by convention it does not exercise this jurisdiction, deferring to the IGIS. Government has agreed to formally remove the Ombudsman's jurisdiction (Government Response to the Comprehensive Review - Recommendation 167).
4. The military components of ASD, DIO and AGO are subject to various ADF oversight measures (including the ADF Inspector-General, the ADF Investigative Service, and the Ombudsman.
5. However, note that the Government has agreed to exempt the ACIC from the FOI Act (Government Response - Recommendation 187), and to remove AGO's current FOI exemption insofar as documents are not related to intelligence functions (Government Response - Recommendation 186).