

Chapter 3

Complaints handling and Ombudsman's findings

3.1 This chapter examines the ongoing management of complaints by the Australian Federal Police (AFP), as well as an overview of the findings of the Commonwealth Ombudsman (the Ombudsman), which has a statutory oversight role of the AFP.

3.2 Examination of the Ombudsman's findings with respect to the AFP is limited to oversight of complaints management and controlled operations, including the use of surveillance devices.

Complaints management

3.3 During 2016–17, the AFP received 421 complaints, a 15 per cent decrease on the previous reporting period (494 complaints).¹ Figure 1 illustrates the trend in the overall number of complaints and alleged breaches from 2010–11 to 2016–17.

Figure 1: Number of complaints and alleged breaches, 2010–11 to 2016–17²



3.4 This figure classifies complaints according to the four categories of conduct for AFP appointees under Part V of the *Australian Federal Police Act 1979* (AFP Act), defined as follows:

1 Australian Federal Police (AFP), *Annual Report 2016–17*, p. 114.

2 AFP, *Annual Report 2016–17*, p. 115.

Conduct issues falling within Category 1 are the least serious and relate principally to customer service. Category 2 complaints relate to minor misconduct and inappropriate or unsatisfactory behaviour. Category 3 complaints relate to serious misconduct that does not give rise to a corruption issue. Category 4 complaints relate to corruption, and these are referred to ACLEI.³

3.5 The AFP's 2016–17 annual report identifies that while the number of overall complaints decreased, the number of serious complaints increased. Category 3 complaints increased by 45 per cent, while Category 4 complaints rose by 32 per cent.⁴

3.6 In its report, the AFP attributes the increase in the number of corruption complaints to a 2013 realignment of the definition of corruption to sit under the Law Enforcement Integrity Act 2006. The AFP also attributes the increase in serious misconduct complaints to a total of 54 complaints relating to credit card misuse.⁵

3.7 The AFP informed the committee that a number of steps have been taken to educate its employees about the new definition of corruption, including the publication of the *AFP Fraud Control and Anti-Corruption Plan* in 2016. This plan outlines a number of processes and procedures aimed at ensuring staff are able to recognise fraud and take appropriate action when required, including (but not limited to):

- recruitment and induction training of all new appointees;
- mandatory online Fraud and Anti-Corruption Control training to be undertaken by all appointees;
- raising managerial awareness of fraud risk at functional and operational levels; and
- reinforcement and behavioural modelling from senior management and executive levels.⁶

3.8 These processes are complimented by ongoing communication of integrity issues through email and postings on the AFP intranet, as well as through early intervention strategies when a complaint arises.⁷

3.9 On notice, the AFP advised the committee that it has since utilised the publication *Our Culture, Our Newsletter*, which is produced by the Workplace Development and Culture Portfolio, to remind AFP staff of their obligations relating to the use and acquittal of corporate credit cards.⁸

3 AFP, *Annual Report 2016–17*, p. 114.

4 AFP, *Annual Report 2016–17*, p. 114.

5 AFP, *Annual Report 2016–17*, p. 116.

6 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), pp. 1–2.

7 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), p. 2.

8 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), p. 3.

3.10 The AFP stated that Category 3 or Category 4 issues are referred to the Professional Standards Panel which comprises senior executive level staff. This panel can determine a sanction which is commensurate with the established behaviour and any relevant mitigating and aggravating factors.⁹ Since June 2018, the de-identified outcomes from such investigations have been published.¹⁰

Committee view

3.11 The committee welcomes the downward trend in the number of complaints and alleged breaches of conduct for AFP appointees. The committee is concerned at the sharp increase in the number of serious misconduct and corruption complaints.

3.12 The committee does, however, recognise that the AFP has taken steps in order to reduce the number of Category 3 and Category 4 complaints, and is reassured by updated statistics provided by the AFP on notice which reflect a decrease in both categories.¹¹ The committee will continue to monitor the number of complaints concerning all four categories of alleged breaches of conduct, but particular attention will be paid to Category 3 and Category 4 complaints.

Ombudsman's report—controlled operations

3.13 Section 15HS(1) of the *Crimes Act 1914* (Crimes Act) provides that:

The Ombudsman must, from time to time and at least once every 12 months, inspect the records of each authorising agency to determine the extent of compliance with this Part [Part IAB—Controlled operations] by the agency and by law enforcement officers.

3.14 The AFP is one such authorising agency.¹²

3.15 Section 10 of the *Parliamentary Joint Committee on Law Enforcement Act 2010* requires the Ombudsman, at least once per calendar year, to brief the committee about the involvement of the AFP and the Australian Crime Commission (ACC) in controlled operations under Part 1AB of the Crimes Act during the preceding 12 months.

3.16 On 3 December 2018, the committee met with representatives from the Ombudsman who briefed the committee in private about controlled operations, including in respect of the Ombudsman's public report on the controlled operations activities of ACLEI, the AFP and the ACC for the period 1 July 2016 to 30 June 2017.

3.17 A *Report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017* was published in

9 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), pp. 2–3.

10 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), p. 3.

11 AFP, answers to written questions on notice, 4 March 2019 (received 18 March 2019), p. 2.

12 *Crimes Act 1914*, s. 15GC.

August 2018.¹³ The report covers the Ombudsman's inspections of the AFP and other law enforcement agencies' records over the period 1 July 2016 to 30 June 2017. Two inspections were conducted at the AFP. These inspections examined controlled operations authorities that expired or were cancelled during the period 1 January 2016 to 30 December 2016.¹⁴

3.18 The Ombudsman found two significant non-compliance issues that had also been raised in the previous reporting period (2015–16).

Authorities granted by the AFP that prescribed activities that could have been authorised under other legislation

3.19 There were two controlled operations which the Ombudsman initially considered could have required authorisation under the *Telecommunications (Interception and Access) Act 1979* (TIA Act). In the 2015–16 reporting period, the AFP advised that they would obtain internal advice prior to authorising controlled operations to prevent a recurrence. During the 2016–17 period, however, the AFP and Attorney-General's Department advised that the activities could not have been authorised under the TIA Act. The Ombudsman has now raised a policy question for the Department of Home Affairs (which now administers Part IAB) as to whether the activities in question should be covered by a warrant regime.

Participants and/or activities of controlled operations that were not authorised

3.20 Six instances where participants, including civilians, and/or activities of a controlled operation were not authorised were identified in 2016–17. This was a reduction from the previous reporting period. The Ombudsman acknowledged the decrease in the number of instances, and the AFP's implementation of recommended training to address the issue.¹⁵

3.21 The Ombudsman's report also made a number of other findings of note.

13 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, http://www.ombudsman.gov.au/_data/assets/pdf_file/0032/88349/Part-IAB-Annual-Report-2016-17.pdf (accessed 23 October 2018).

14 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, p. 10.

15 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, pp. 15–16.

Standard authority granted for operation meeting the threshold of a major controlled operation

3.22 The Ombudsman identified one instance of this, which was acknowledged as an issue by the AFP. The AFP stated it would update its policy guidance to prevent further instances.¹⁶

Urgent authority granted for controlled operation previously subject to formal authority

3.23 There was one instance where the AFP wrongly granted an oral authority for an operation already granted formally. The AFP is reported to have taken remedial action to prevent a recurrence.¹⁷

Authorities not varied in accordance with Part IAB

3.24 There were a number of instances where new authorisations were granted rather than variations to existing authorisations. There was one instance where the AFP varied to include conduct that targeted a different criminal offence than what was stated on the original authority; this is not permitted under s15GO of the Crimes Act. The effect of these non-compliant variations is that they escape scrutiny by the Administrative Appeals Tribunal (AAT). The Ombudsman advised the AFP not to seek new authorities where existing ones could be varied. The AFP acknowledged the issue and amended its guidance material, including information in relation to the AAT oversight role.¹⁸

Committee view

3.25 The committee thanks the Ombudsman for the private briefing it received about the AFP's exercise of its controlled operations powers during the reporting period.

3.26 The committee supports the Ombudsman's findings and acknowledges that the AFP has implemented responses in relation to the Ombudsman's earlier recommendations in relation to controlled operations. It is of particular note that the AFP has implemented training and professional development to ensure greater compliance with controlled operations regulations. However, noting that there are some ongoing issues in relation to controlled operations, the committee will continue to pay particular attention to the AFP's performance in this regard.

16 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, p. 12.

17 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, pp. 12–13.

18 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's activities in monitoring controlled operations for the period 1 July 2016 to 30 June 2017*, August 2018, pp. 13–15.

Ombudsman's report—surveillance devices

3.27 Pursuant to section 55 of the *Surveillance Devices Act 2004* (SD Act):

The Ombudsman must inspect the records of a law enforcement agency to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency.¹⁹

3.28 The AFP is one such law enforcement agency.²⁰ The *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 July to 31 December 2017*²¹ was published in March 2018; for the period 1 January to 30 June 2018 the report was published in September 2018.²² The most recent report was the first to be presented to the Minister for Home Affairs, as amendments were made to the Administrative Arrangements Order in May 2018 transferring responsibility for the administration of the SD Act from the Attorney General to the Minister for Home Affairs.²³

3.29 The March 2018 report states that an inspection of the AFP's surveillance device (SD) records was made in March 2017 for the inspection period 1 July to 31 December 2016. The inspection covered 65 of the 496 SD warrants issued to the AFP, as well as 10 of the 21 tracking device authorisations that had expired or been revoked during the period 1 July to 31 December 2016.²⁴

3.30 The Ombudsman did not make any recommendations based on its inspection of the AFP's records. The Ombudsman did, however, identify some issues for consideration by the AFP:

- use and retrieval of SDs without proper authority; and
- non-compliance with destruction and retention provisions of the SD Act.²⁵

3.31 These errors were identified as being administrative in nature, and the AFP advised that guidance material had been amended and issued.²⁶

19 *Surveillance Devices Act 2004*, s. 55(1).

20 *Surveillance Devices Act 2004*, s. 6A(6).

21 Commonwealth Ombudsman, *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 July to 31 December 2017*, March 2018, http://www.ombudsman.gov.au/data/assets/pdf_file/0034/85498/664056_Ombudsman_Report-1-PDF-PROOF.PDF (accessed 23 October 2018).

22 Commonwealth Ombudsman, *Report to the Minister for Home Affairs on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 January to 30 June 2018*, September 2018, http://www.ombudsman.gov.au/data/assets/pdf_file/0026/89603/Surveillance-Devices-Six-Monthly-Report-to-Home-Affairs-September-2018.pdf (accessed 23 October 2018).

23 Commonwealth Ombudsman, *Report to the Minister for Home Affairs on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 January to 30 June 2018*, September 2018, footnote 3, p. 2.

24 Commonwealth Ombudsman, *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 July to 31 December 2017*, March 2018, p. 9.

25 Commonwealth Ombudsman, *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 July to 31 December 2017*, March 2018, p. 9.

Committee view

3.32 The committee is satisfied by the Ombudsman's conclusion that the AFP has taken appropriate remedial action to address the administrative issues identified as a result of the inspections.

Ombudsman's report—stored communications and telecommunications data

3.33 Pursuant to s 186B of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the Ombudsman is empowered to conduct inspections of specified law enforcement agencies that can access an individual's stored communications and/or telecommunications data when investigating certain offences.²⁷

3.34 The AFP is one such agency.²⁸

3.35 The Ombudsman conducted 37 inspections of agencies' access to telecommunications during 2016-17, including the AFP. As a result of these inspections, the Ombudsman concluded that the agencies were generally exercising their power to access telecommunications data appropriately.²⁹ There were, however, a number of key issues identified in the course of the inspections.

3.36 One issue concerned the requirements under s 180H of the TIA Act with respect to Journalist Information Warrants. This was the subject of the Ombudsman's routine inspection of the AFP and a further inspection on 5 May 2017. The findings of both inspections are discussed in paragraphs 3.36 to 3.42 below.

3.37 The Ombudsman became aware, by way of disclosure from the AFP, of authorisations to disclose telecommunications data made by an officer within ACT Policing who did not have the authority to do so under s 5AB(IA) of the TIA Act. This affected 116 authorisations. The AFP attributed these errors to administrative oversight. The Ombudsman suggested that the telecommunications data obtained under these authorisations be quarantined, which was accepted by the AFP but not acted on at the time. The data was subsequently further used and communicated, but was partially quarantined in February 2018 following an inquiry by the Ombudsman. The Ombudsman was satisfied with the prompt remedial action which was taken

26 Commonwealth Ombudsman, *Report to the Attorney-General on agencies' compliance with the Surveillance Devices Act 2004 for the period 1 July to 31 December 2017*, March 2018, p. 10.

27 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, November 2018, http://www.ombudsman.gov.au/_data/assets/pdf_file/0033/96747/201617-Chapter-4A-Annual-Report.pdf (accessed 7 March 2019), p. 1.

28 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, November 2018, p. 6.

29 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, November 2018, pp. 1–2.

following the identification of this breach, but will continue to monitor this issue closely with the AFP.³⁰

Committee view

3.38 The committee supports the Ombudsman's findings and is satisfied that the AFP has taken appropriate remedial action to address the administrative issues identified during the inspections and subsequently with respect to the quarantine of information.

Ombudsman's report—Access to journalist's telecommunications data without a Journalist Information Warrant

3.39 On 26 April 2017, the AFP advised the Ombudsman's office of a breach of the TIA Act. The breach occurred when AFP officers accessed metadata pertaining to a journalist without obtaining a Journalist Information Warrant as required under s 180H of the TIA Act.³¹

3.40 The Ombudsman conducted an inspection on 5 May 2017. The findings that arose out of that inspection were the subject of a report dated October 2017.³² The AFP found that there were four relevant authorisations in question, one of which was a clear breach, while the status of the remaining three alleged breaches were 'arguable'.³³

3.41 The Ombudsman identified four main contributing factors which led to the breach:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within PRS
- within PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers
- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing applications that did not meet relevant thresholds from being progressed

30 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, November 2018, pp. 10–11.

31 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, http://www.ombudsman.gov.au/_data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf (accessed 7 March 2019), p. 4.

32 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017.

33 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 9.

-
- although guidance documents were updated prior to the commencement of the Journalist Information Warrant provisions, they were not effective as a control to prevent this breach.³⁴

3.42 While the Ombudsman acknowledged that the AFP had 'responded appropriately' to the breach,³⁵ it made one key recommendation:

[t]hat the Australian Federal Police immediately review its approach to metadata awareness raising and training to ensure that all staff involved in exercising metadata powers have a thorough understanding of the legislative framework and their responsibilities under Chapter 4 of the Telecommunications (Interception and Access) Act 1979.³⁶

3.43 In response, the AFP advised the Ombudsman that it was finalising a training package that all AFP authorised officers would need to undertake as a prerequisite to maintaining their authorised officer status each year.³⁷

3.44 The Ombudsman also made a number of suggestions in respect of strengthening existing controls. The AFP advised that some of these had been implemented and would turn its attention to implementing the remaining suggestions.³⁸

3.45 The Ombudsman stated that it would continue to monitor the AFP's compliance with the TIA Act and its progress on previous inspection findings through its routine annual inspections.³⁹

34 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 11.

35 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 9.

36 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, pp. 14, 19.

37 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 19.

38 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 19.

39 Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, p. 19.

Committee view

3.46 The committee supports the Ombudsman's findings and recommendation. It acknowledges that the AFP has undertaken steps to remedy the breach and to increase its officers' awareness of the requirements of s 180H of the TIA Act to prevent a reoccurrence. The committee is eager to hear the outcome of the Ombudsman's ongoing monitoring of the AFP's compliance with the TIA Act, and its implementation of the findings of the Ombudsman's report.

Mr Craig Kelly MP
Chair