Chapter 3

Reports on the operation of acts and programs

3.1 Standing Order 25(20) does not provide for the consideration of reports on the implementation or operation of acts or programs. The committee is not required to include them in its report on the examination of annual reports; however, as on previous occasions, the committee has chosen to examine such reports, specifically the:

- *Surveillance Devices Act* 2004 Annual Report 2014–15; and
- *Telecommunications (Interception and Access) Act 1979* Annual Report 2014–15.

Report on the operation of the *Surveillance Devices Act 2004*

3.2 The annual report on the operation of the *Surveillance Devices Act 2004* (SD Act) was tabled in the Senate on 15 June 2015.[1] The report relates to the period from 1 July 2014 to 30 June 2015.

3.3 The report noted that during the 2014–15 reporting period, there were no significant policy developments or amendments to the SD Act. Furthermore, there were no significant judicial decisions.[2] In 2014–15, there was an increase of 2 per cent in warrants being issued under the SD Act. This was a modest increase compared to the 16 per cent increase in the previous reporting period (2013–14).[3]

3.4 The executive summary of the SD Act annual report highlighted the role of the SD Act had played in securing convictions. In 2014–15, information obtained under the SD Act contributed to convictions in 76 cases. This number of convictions was an increase over 50 per cent from 2013–14. Historical data was provided from 2004–05 and indicated a mostly upward trend in the number of convictions.[4]

Applications for surveillance device warrants

3.5 Only eligible judges from the Family Court of Australia, the Federal Court and the Federal Circuit Court, or a nominated AAT member, are able to issue a surveillance device warrant. The total number of judges and AAT members available to issue a SD warrant in 2014–15 was 79, with 32 of those being Federal Circuit Court judges. Overall, this total continued a downward trend from 96 in 2012–13 and 84 in 2013–14.[5]

---

1 *See Appendix 1*, p.25.

2 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 9.

3 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 9.

4 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 2.

5 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 5.

3.6 Not all of the data in relation to the number of warrants obtained at the state and territory level was available. State and territory law enforcement agencies generally rely on their own legislative regimes for the use of surveillance devices, although they are able to make use of the SD Act when dealing with a Commonwealth matter or during a joint operation.[6]

3.7 Pursuant to paragraph 50(1)(a) of the SD Act, the annual report must provide information on the number of applications for warrants made and the number of warrants issued for the reporting period. Under subsection 50(2), the SD Act also requires the report to provide a breakdown of these numbers in respect of each different kind of surveillance device.[7]

3.8 For 2014-15, law enforcement agencies made applications for 876 warrants, and 875 warrants were issued by an eligible judge or nominated AAT member. One warrant was not issued due to insufficient information being provided to the judge or AAT member.[8]

3.9 Table 3.1 provides a breakdown of the warrants issued by agency for 2012–13, 2013–14 and 2014–15.[9]

6 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 9.

7 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 11.

8 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 11.

9 Adapted from: AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 12.

Table 3.1

Agency	2012–13	2013–14	2014–15
Australian Crime Commission (ACC)	166	211	266
Australian Commission for Law Enforcement Integrity (ACLEI)	6	14	2
Australian Federal Police (AFP)	557	622	606
CCC (QLD)	2	7	–
WA Police	–	2	1
SA Police	4	–	–
VIC Police	2	–	–
Total	737	856	875

3.10 Section 15 of the SD Act provides for remote application for a warrant. A remote warrant could be made by telephone, fax, email or other means of communication if it is impracticable for the law enforcement agency to apply in person. In 2014–15, the AFP applied remotely for and was issued two surveillance device warrants.[10]

3.11 Section 19 of the SD Act allows for a law enforcement officer to apply for an extension for a 'warrant for a period not exceeding 90 days after the warrant's original expiry date'.[11] In 2014–15, no applications were refused and 152 applications were submitted, 23 more than 2013–14.[12]

3.12 The Annual Report stated that there were 11 emergency authorisations issued to the AFP in 2014–15; no authorisations of this type have been issued in the past two years.[13] Emergency authorisations can be issued 'in cases of serious risk to person or property…urgent circumstances relating to a child recovery order…or where there is a risk of loss of evidence'.[14]

10 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 14.

11 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 14.

12 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 14.

13 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 15.

14 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 15.

3.13 The SD Act requires that the annual report must provide data on the number of applications for tracking device authorisations and the number of tracking device authorisations given. The table below is extracted from the report[15]:

Table 3.2

Agency		2012–13	2013–14	2014–15
Australian Crime Commission (ACC)	Applications	10	12	21
	Authorised	10	12	21
Australian Federal Police (AFP)	Applications	56	58	56
	Authorised	56	58	58
Total		66	70	77

3.14 Section 50 requires the inclusion of information which is, for the committee's purpose, indicative of the SD Act's effective use, such as: the number of arrests; prosecutions and convictions; as well as 'the number of locations and safe recoveries of children', based on information obtained using surveillance devices.[16]

3.15 The following table shows the number of arrests, prosecutions and convictions for 2014–15. The figures in brackets refer to the preceding reporting period 2013–14.[17]

Table 3.3

AGENCY	Arrests	Safe Recovery	Prosecutions	Convictions
ACC	(49) 38	–	(12) 1	(–) 1
AFP	(154) 123	–	(128) 135	(35) 71
CCC (QLD)	(1) 3	–	–	–
Victoria Police	(–) –	–	(–) 4	(–) 4
Total	(204) 164	–	(140) 140	(35) 76

3.16 The report noted that information regarding arrests, prosecutions (inclusive of committal proceedings) and convictions should be interpreted with caution, especially

15 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 16.

16 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 16.

17 Adapted from: AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2014*, p. 18.

in presuming a relationship between them. An arrest in one reporting period might not lead to a prosecution in a later reporting period, likewise a conviction in one reporting period could be recorded in another period. Further, there is no correlation between the number of charges and arrests as an arrest could lead to conviction for multiple offences. Also, in situations where the weight of evidence obtained from surveillance devices is sufficient for defendants to enter guilty pleas, it may not be necessary for surveillance information to be introduced as evidence.[18]

Telecommunications (Interception and Access) Act 1979

3.17 The annual report for 2014–15 on the *Telecommunications (Interception and Access) Act 1979* (TIA Act) was tabled in the Senate on 17 June 2015.[19]

3.18 Section 104 of the TIA Act sets out the provisions for annual reports, specifically:

> The Minister shall cause a copy of a report under section 93 or Division 2 to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives the report, or the report is prepared, as the case may be.[20]

3.19 The committee notes that the report was tabled before the required date in both Houses of Parliament.

3.20 The TIA Act has the primary goal of protecting the privacy of individuals who use the Australian telecommunications network. Communications cannot be intercepted unless authorised by specific circumstances set out in the TIA Act. Law enforcement agencies have the option to access several separate warrants to intercept a communication. These include warrants for real-time content and for stored communications.[21]

3.21 From 13 October 2015, the TIA Act limited the number of agencies that are able to access stored communications. This restriction allows for only criminal-law enforcement agencies and the Commonwealth Ombudsman to access this information via the TIA Act. This change was a product of the passing of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act). The Data Retention Act obliges carriers to retain specific information for a period of two years. In addition to the retention of data and the reduction in the number of agencies that have access to this information, the Data Retention Act also imposes additional record keeping and reporting obligations for those law enforcement agencies that wish to access telecommunications data.[22]

---

18 AGD, *Surveillance Devices Act 2004 Report for the year ending 30 June 2015*, p. 17.

19 *See Appendix 1*, p.25.

20 *Telecommunication (Interception and Access) Act*, s. 104(1).

21 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. V.

22 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. V.

3.22 This annual report does not include those additional reporting requirements implemented by recent changes to the TIA Act; these reporting requirements will be in place in the 2015–16 annual report.[23]

3.23 In 2014–15 interception warrants were available to 17 Commonwealth and state and territory agencies including the ACC, ACLEI, AFP, state and territory police and state anti-corruption agencies.[24] In order to use an interception warrant an authority must be satisfied that the agency is investigating a serious offence. A serious offence is generally a crime committed that carries a penalty of at least seven years' imprisonment.[25]

3.24 The report noted that an interception warrant may only be issued by an eligible judge or a nominated AAT member. Eligible judges in 2014–15 included members of the Federal Court of Australia, the Family Court of Australia and the Federal Circuit Court. Judges have to be declared eligible by the Attorney-General and formally consent in writing to be an eligible judge.[26]

3.25 During the reporting period a total of 3926 telecommunications interceptions warrants were issued by judges and nominated AAT members (see table 3.4).[27]

Table 3.4

Issuing Authority	**Family Court Judges**	**Federal Court Judges**	**Federal Circuit Court Judges**	**Nominated AAT members**	**Total**
Number of warrants issued	204	241	258	3223	3926

3.26 Table 3.5 shows the number of applications for warrants, telephone applications for warrants and renewal applications that were made, withdrawn and issued. The figures in brackets refer to the preceding reporting period 2013–14.[28]

23 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. V.

24 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 1.

25 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 2.

26 AGD, *Telecommunications (Interception and Access) Act annual report 2014-15*, p. 4.

27 Adapted from: AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 5.

28 Adapted from: AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 7.

Table 3.5

	Applications for warrants	**Telephone Applications for Warrants**	**Renewal applications**
Made	(4025) 3935	(75) 45	(603) 750
Refused/withdrawn	(18) 9	(–) –	(–) –
Issued	(4007) 3926	(75) 45	(603) 750

3.27 The report's key findings noted the information obtained under these warrants led to 3100 arrests, 4686 prosecutions and 1912 convictions.[29]

Stored communications

3.28 The TIA Act enables law enforcement agencies to apply for stored communications warrants to assist investigations. These warrants may apply to email, SMS or voice message communications.[30]

3.29 Table 3.6 shows the number of applications for warrants, telephone applications for warrants and renewal applications that were made, withdrawn and issued. The figures in brackets refer to the preceding reporting period 2014–15.[31]

Table 3.6

	Applications for stored communications warrants	**Telephone Applications for stored communication warrants**
Made	(572) 697	(1) 0
Refused/withdrawn	(1) 1	(0) 0
Issued	(571) 696	(1) 0

3.30 During the reporting period, law enforcement agencies made 377 arrests, undertook 335 proceedings and made 198 convictions based on evidence obtained under stored communications warrants.[32]

29 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, pp VII-VIII.

30 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 31.

31 Adapted from: AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 33.

32 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15*, p. 34.

Telecommunications data

3.31 Chapter four of the TIA Act allows enforcement agencies to access 'telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue'.[33]

3.32 The report noted that 83 enforcement agencies made historical data authorisations[34] and 354 841 data authorisation to enforce the criminal law.[35] The number of authorisations has increased by 30 581 compared to 2013–14 (324 260 authorisations).[36]

Senator the Hon Ian Macdonald
Chair

33 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15,* p. 41.

34 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15,* p. 41.

35 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15,* p. 42.

36 AGD, *Telecommunications (Interception and Access) Act annual report 2014–15,* p. 44.