Tim McCulloch
Barrister

FOLEY'S LIST

Telephone Intercepts and Surveillance Device Warrants

Introduction

1. Evidence derived from telephone intercepts (TIs) and surveillance devices (SDs) is a common feature of criminal prosecutions. This type of evidence is particularly common in offences that have a federal connection, such as drugs and terrorism. But how common are they?

2. In 2020-21 Victoria Police applied for 250 SD warrants[1] under the Victorian Act[2].

3. Nationally, there were 830 SD warrants sought under the Cth Act, of which some 750 were sought by the AFP. None were sought by Victoria Police.[3] Various other bodies such as IBAC and ICAC are also empowered to seek SD warrants under the state and federal legislation.

4. By contrast, in 2019-20, nationally it appears there were some 4320 telephone intercept warrants issued, of which 2096 related to serious drug offences. Only 50 of those were sought by Victoria Police, compared to 816 by NSW Police and 464 by the AFP.[4]

5. Whilst those figures do not appear large at first blush, the evidence derived from TI and SD sources can be extensive and may affect a large number of individual prosecutions, particularly in the area of drug offences.

6. Warrants authorising the collection of this information should be scrutinised carefully.

---

[1] To put that in context, the Public Interest Monitor appeared on 270 "relevant applications" in total in the 2020-21 calendar year. That number includes applications under the Telecommunications (Interception and Access) Act 1979 (Cth), *Major Crime (Investigative Powers) Act* 2004 and other Acts. See - https://parliament.vic.gov.au/file_uploads/Public_Interest_Monitor_Annual_Report_2020-21_p0qvydGW.pdf

[2] Note – it appears that this figure covers all branches of VPOL including Professional Standards and OCE where the VPOL Annual Report (See Appendix 1) only refers to 70 applications

[3] https://www.homeaffairs.gov.au/nat-security/files/surveillance-devices-act-2004-annual-report-2020-21.pdf

[4] https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-19-20.pdf

Telephone Intercepts

7. As the figures above demonstrate, telephone intercepts are far more prevalent than surveillance devices.

8. Given that telecommunications are an area of exclusive federal jurisdiction, the *Telecommunications (Interception and Access) Act* 1979 (Cth) covers the field regarding the issue of TI warrants.

9. A few definitions:

    a. 'Serious offences' are defined at s 5D as including murder, kidnaping and various other serious offences against the *Criminal Code*.
        i. 5D goes onto include all offences punishable by 7 years or more imprisonment, that also involve loss of life or serious injury, or risk of same, serious damage to property and arson, trafficking in drugs, fraud bribery and tax evasion amongst others.
        ii. Suffice to say that a wide array of state and commonwealth offences are captured.
    b. Section 6 - Interception of communication consists of listening to or recording…a communication in its passage over [a] telecommunications system <u>without the knowledge of the person making the communication.</u>[5]

10. Section 7 sets out a general prohibition on the interception of telecommunications without warrant.

11. Telecommunications Service Warrants may be issued by eligible judges or nominated AAT members:

    a. An eligible judge is one who has provided a written consent and who the Attorney General has made a declaration in relation to;[6]
    b. A nominated AAT member is one who has been nominated in writing by the AG, and who is a Deputy President, senior member or member of the AAT. The AG must not nominate a part-time member unless they are an enrolled legal practitioner of more than 5 years experience.[7]

[5] The common query is whether it is unlawful for one party to a telephone call to record the conversation at their end. The answer is no, as they are not intercepting the call and are a recipient.
[6] Section 6D
[7] Section 6DA

Table 1: Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges, and nominated AAT members to issue warrants.

Issuing authority	Number		
	18/19	19/20	20/21
Nominated AAT Members	33	36	36
Family Court Judges	9	10	10
Federal Circuit Court Judges	36	32	32
Federal Court Judges	15	13	13
TOTAL	**93**	**91**	**91**

[8]

12. To be an 'agency' capable of seeking a warrant under the Act, an eligible authority (such as Victoria Police) must be declared to be an agency under section 39.

13. The form of application is prescribed by s 40, and unless in an emergency situation, it must be made in writing, supported by affidavit (section 42).

14. Section 44A provides legislative force for the role of the Victorian PIM (see below) in relation to these federally issued warrants.

15. Sections 46 and 46A govern the issue of Telecommunication Service Warrants, or Named Person Warrants. The threshold for issue of a warrant is:

    a. Compliance with the procedural matters in Division 3;
    b. **Reasonable grounds for suspecting that a particular person is using or likely to be using the [telephone] service** (or in the case of 46A is likely to be using more than one telecommunications service;
    c. **Information would be obtained under the warrant…that would assist in the investigation… of a serous offence or offences**…in which a particular person is involved...or another person is involved with whom the particular person is likely to communicate using the service.

16. A warrant may target a person or a telephone service. And it may target a service that is not only used by the person, but one with which the person may communicate (perhaps their spouse or associate).

17. The judge or AAT member is required to consider the matters in 46(2) or 46A(2). These include the impact on privacy of persons, gravity of offence being investigated, how likely the information is to assist, other methods already used, whether other available methods would assist, whether those methods would prejudice the investigation, submissions of the PIM.

[8] https://www.homeaffairs.gov.au/nat-security/files/surveillance-devices-act-2004-annual-report-2020-21.pdf

18. Pay close attention to section 49 – Form and Content of warrant. The warrant must be:

    a. In the prescribed form and signed;
    b. May be up to 90 days, may not be extended;
    c. Must set out the short particulars of each serious offence to which it relates;[9]

19. In practice specific officers will monitor intercepted communications and generate call summaries which are passed to investigators alongside the recorded communication. Communications which are of nil value, are outside the scope of the warrant or are privileged are [meant to be] quarantined from the investigating officer.

Surveillance Device Warrants

20. There are two legislative sources for the power to issue SD warrants. The first is the *Surveillance Devices Act 2004* (Cth) and the second is the *Surveillance Devices Act* 1999 (Vic).

21. I will focus on the Victorian Act. The provisions defining surveillance devices are on par as between the Vic and Cth Acts. The thresholds for issuing a Commonwealth SD warrant and the mandatory considerations at time of issue are closely aligned with what is found in the TI Act Cth (set out above). [10]

22. A few definitions:

    a. SDs may be issued in relation to a "relevant offence" which is defined as:
        i. An offence punishable by 3 years or more; or
        ii. An offence that has been prescribed by regulation under the Act.
    b. A SD is defined as a data surveillance device, listening device, optical surveillance device or a tracking device; or any device that is a combination of any of the above;
    c. An OSD is any device capable of being used to visually record an activity (not including spectacles or other devices used to overcome vision impairment);
    d. An LD, is unsurprisingly a device capable of being used to overhear, record or monitor a conversation or words (not including hearing aids);
    e. Tracking device is any which is capable of being used to determine or monitory the location of a person or object.

[9] Does not have to contain the same level of clarity as an indictment.
[10] As the figures set out above, where there is a serious offence with a federal aspect, those matters tend to be almost exclusively investigated by the AFP.

23. The Vic Act, sets up the general prohibition on the use of SDs at sections 6 to 8 and does this by reference to 'private activity' and 'private conversations'. Any security camera would be caught by this provision if not for the definition of private activity, which excludes any activity carried on outside a building, where one would argue that there is no reasonable expectation of privacy. There is a general prohibition on the use of tracking devices without express or implied consent.

24. An investigatory authority is not likely to require a warrant to install a listening device or a camera in a public place. But from a practical perspective a warrant is always required to authorise entry on to premises which would otherwise be a trespass or to authorise entry into a private vehicle in circumstances that would otherwise be unlawful.

25. SD warrants and retrieval warrants may be issued by a judge of the Supreme Court of Victoria (s 14)[11]. At the federal level, SD warrants may be issued by a Judge of the Federal Court, of the Federal Circuit and Family Court, a nominated member of the AAT. See more on this topic in TIs.

26. Section 15 sets out the procedure for seeking a warrant. The threshold is that the "law enforcement officer [suspects] on reasonable grounds that *an offence has been or is about to be committed; and the use of the surveillance device is or will be necessary for the purpose of an investigation in that offence or of enabling evidence or information to be obtained of the commission of that offence or of the identity or location of the offender.*"

27. Application may only be made with the approval of a senior officer of the relevant agency or an authorised police officer.[12] In practice, all applications must be in writing and supported by an affidavit, expect in emergency situations, but the figures disclose that the emergency power is rarely used and it requires the court to validate the use of the power within 48 hours. All applications must be provided to the Public Interest Monitor.

28. There is presently one PIM and two deputy PIMs. The PIM is empowered to make submissions generally in writing, or orally, and may engage in discussions with the applicant regarding the scope of the warrant. In practical terms when the various statutory annual reports are reviewed, a refusal to issue a warrant by the Supreme Court is exceptionally rare.

29. Section 17 requires that a judge be satisfied that there are reasonable grounds for the suspicion or belief in the application and must have regard to the:

[11] Magistrates may also issue warrants for tracking devices only – [s 15(3)(b)] but in practical terms they tend to be issued by the Supreme Court.

[1212] There is a process established for the Chief Commissioner to approved nominated officers under the Act.

a. Nature and gravity of the alleged offence
b. Extent to which privacy of any person is likely to be affected;
c. Alternative means of obtaining the evidence;
d. Evidentiary or intelligence value of the evidence
e. Any previous warrant;
f. Submissions made by the PIM

30. Section 18 sets out what the warrant must contain. It is too lengthy to set out here, but pay close attention to the date of issue of the warrant, it must be signed, the alleged offence in relation to which the warrant is issued must be stated clearly, the description of the premises or object (such as a car) in relation to which the SD is authorised must also be clear and unambiguous. SD warrants may not exceed 90 days but may be extended under s 20, subject to the same considerations already set out.

31. According to s 19, an SD warrant authorises, the use of an SD on premises, in an object, or in respect of the "*the conversations, activities or geographical location of a specified person or a person who's identity is unknown.*"

Challenging a warrant on its face

32. There are very limited circumstances where you may be able to go behind the warrant, and seek access to the affidavit itself as a means of attacking the grounds on which it was issued – see for *example R (Cth) v Petroulias (No 8)* [2007] NSWSC 82, - where it was alleged that the Assistant Commissioner of Taxation have provided false information to AFP officers, who had then relied on that information in the affidavit seeking a warrant. That application failed as the *male fides* were found not to exist, however the court did observe that those seeking a warrant must be "*scrupulous to ensure that the contents of the affidavit fully and accurately*" set out the factual basis for the issue of the warrant.

33. Absent that rare situation, your attention should be on whether:

a. The warrant is valid on its face; and/or
b. The warrant and its objective scope were complied with by executing officers.

34. In *George v Rockett*[13], the High Court observed that in prescribing conditions governing the issue of search warrants the legislature has sought to balance the need for an effective criminal justice system against the need to protect the individual from arbitrary invasion of their privacy. A person's interest in privacy is recognised in all modern bills of rights and it has achieved a status in international human rights law.

[13] [1990] HCA 26 (20 June 1990)

35. A warrant is to be construed objectively. Meaning that the following matters are generally irrelevant:

    a. What the applicant for the warrant subjectively intended;
    b. What the issuer of the warrant subjectively intended or understood; or
    c. The nature of the evidence giving rise to the issue of the warrant.

36. You may have regard to the legislation that underpins the issue of the warrant to aid in interpreting it, but that will not save a warrant that is fatally ambiguous. For example, in the case of pro-forma warrants issued under the Victorian *Crimes Act* or DPCSA it is not unheard of for the applicant to fail to complete sections of the warrant, meaning that it objectively authorises nothing.

37. The warrant must adequately describe the offence alleged. If a warrant fails to do so, it may be held to be invalid

38. This was recently discussed in the High Court in the matter of Annika Smethurst, a News Limited journalist whose home was raided after reporting on matters related to the Australian Signals Directorate.[14] In that case, the High Court discussed, the need for the warrant to adequately state the nature of the offence, by reference to the common law's refusal to countenance the issue of general warrants[15].

39. At [24] the Court refers to the purpose of these provisions to be "*ensuring that each of the issuing officer, the officer executing the warrant and the persons affected by it, understand what is the object of the search and the limits to it*".

40. In that case, the warrant failed to adequately describe the offence to which it related and had the effect of conflating an exclusionary provision with an element of the offence. The warrant was held to be invalid.

41. You should check the warrant for any error on its face, which may lead to invalidity. Either by reference to s 18 of the *Surveillance Devices Act* 1999 (Vic), s 17 of the *Surveillance Devices Act* 2004 (Cth) or s 49 of the *Telecommunications (Interception and Access) Act* 1979 (Cth).

42. If the warrant is valid on its face, consider, what is the scope of what the warrant objectively authorised? Do the particulars of the serious offence alleged in the warrant marry up with the activity alleged in the prosecution brief?

[14] Smethurst v Commissioner of Police [2020] HCA 14
[15] Ibid at [22]

43. As Justice Kyrou stated in *Slaveksi v State of Victoria & Ors*[16], "a search warrant must be executed strictly in accordance with its terms." An example, to illustrate the point – in the case of *R v Applebee*[17] a warrant issued under the Cth Crimes Act authorised search and seizure of two allegedly stolen air compressors. A large number of items were seized under the warrant, demonstrating that the search went far beyond what would have been required to locate two large air compressors. The scope of the warrant was not observed.

44. Equally, one might be able to hypothesise a situation whereby a warrant is issued under Cth legislation authorising telephone intercepts seeking to gain evidence of say, an alleged people smuggling operation.

    a. Where the intercepts disclosed no evidence of any such operation but provided a chance discovery of an unrelated drug trafficking operation, it would be necessary for investigators to return to court and seek a new warrant authorising intercepts relevant to the newly identified offence.
    b. If investigators remained live on that intercept for 90 days seeking evidence of the newly discovered offence, it is likely that they will have exceeded the scope of the warrant.

45. Finally, and more rarely, was there any illegality or other impugned conduct in the execution of the warrant which may give rise to an argument under s 138 that that the evidence was obtained improperly and ought to be excluded.

46. Some practitioners may be aware of the recent 'IT issue' identified by Victoria Police in their monitoring of TI warrants[18]. As discussed above, specific officers generally monitor intercepted communications and generate call summaries. Where an intercepted call is subject to LPP, the recorded call is quarantined and not released to investigating officers.

47. It was discovered that VPOL's IT was set up in such a way that the legally privileged call summaries (but not the intercepted calls) may have been available to investigating officers. In theory, if it could be shown[19], in any affected matter that investigators had accessed the call summaries to which they were legal not entitled, and used that information to further their investigation, it could be argued that the warrant has been contravened, leading to illegality or impropriety and invoking s 138. [20]

Conclusion

[16] [2010] VSC 441 at [156]
[17] (1995) 79 A Crim R 554.
[18] https://www.theage.com.au/national/victoria/bugged-lawyers-conversations-available-to-police-thanks-to-it-error-20201123-p56h4w.html
[19] It was not clear whether this had actually occurred in any specific case and it is not suggested that there have in fact been any such cases
[20] No such cases have arisen as far as I am aware so far.

48. Pay attention to the form and content of a warrant. Ensure that all of the formalities and procedural aspects are valid as a pre-condition to assessing the admissibility of the evidence in a prosecution.

Tim McCulloch

Stawell Chambers

23 February 2022

Appendix 1: Victoria Police 2020-21 Annual Report to Minister under Surveillance Devices Act

ANNUAL REPORT 2020/2021

1. Applications for warrants – Section 30L(1)(a)	Results
1.1 The number of applications for warrants	70
1.2 The number of warrants issued	68

1A. Devices included in issued warrants – Section 30L(2)	Number of devices
1A.1 Data Devices	4
1A.2 Listening Devices	58
1A.3 Optical Devices	14
1A.4 Tracking Devices	40

2. Applications for emergency authorisations – Section 30L(1)(b)	Results
2.1 The number of applications for emergency authorisations	1
2.2 The number of emergency authorisations given	1

2A. Devices included in emergency authorisations – Section 30L(2)	Number of devices
2A.1 Data Devices	0
2A.2 Listening Devices	0
2A.3 Optical Devices	0
2A.4 Tracking Devices	1

3. Remote Applications for warrants – Section 30L(1)(c)	Result
3.1 The number of remote applications for warrants	0

4. Warrants / Emergency authorisations refused – Section 30L(1)(d)	Result	Reason
4.1 The number of warrants that were refused	2	The court took into account the requirements under section 17 d was not satisfied the warrants should be issued.
4.2 The number of emergency authorisations refused	0	N/A

Appendix 2 – 2020-21 Annual Report under the Surveillance Devices Act (Cth)

Key statistics

- In 2020–21, information obtained under the SD Act contributed to 371 arrests, 50 prosecutions, and 42 convictions.
- In 2020–21, 5 law enforcement agencies were issued 830 surveillance device warrants, an increase of 67 from the 763 issued in 2019–20. Three applications for surveillance device warrants were refused by nominated AAT members.
- 367 applications to extend surveillance device warrants were granted, a decrease of 91 from the 458 granted in 2019-20. Applications to extend warrants are often required due to the prolonged nature of investigations for complex and serious crime (where evidence gathering may not have been completed within 90 days).
- 17 retrieval warrants were issued to law enforcement agencies in order to retrieve a lawfully installed surveillance device in 2020–21, a decrease of 3 from the 20 issued in 2019–20.
- 49 tracking device authorisations were issued in 2020-21, a decrease of 51 from the 100 issued in 2019-20. One tracking device retrieval authorisation was issued, the same number as in 2019-20.
- 23 computer access warrants were issued to law enforcement agencies during 2020-21, an increase of 3 from the 20 issued in 2019-20.

Appendix 3 – Telecommunications (Interception and Access) Act 1979 Annual report 2019-20

Table 1: Categories of serious offences specified in telecommunications interception warrants – paragraphs 100(1)(f), 100(1)(g), 100(2)(f) and 100(2)(g)

Categories of offences	ACIC	ACLEI	AFP	CCC (WA)	IBAC	ICAC (NSW)	ICAC (SA)	LECC	NT Police	NSW CC	NSW Police	QLD CCC	QLD Police	SA Police	TAS Police	VIC Police	WA Police	TOTAL
Administration of justice / government offences	-	5	17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**22**
Assisting person to escape or dispose of proceeds	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	**1**
Bribery, corruption and dishonesty offences	-	-	13	41	23	7	17	11	-	-	29	9	6	2	-	-	5	**163**
Cartel offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Child abuse offences	-	-	14	-	-	-	-	-	-	-	1	-	-	-	-	1	-	**16**
Conspire/aid/abet serious offence	16	-	-	-	-	-	6	-	-	-	16	-	-	2	-	5	-	**45**
Cybercrime offences	-	-	8	-	-	-	-	-	-	-	4	-	-	-	-	-	-	**12**
Espionage and foreign interference	-	-	3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**3**
Kidnapping	-	-	1	-	-	-	-	-	-	-	66	-	-	1	-	-	1	**69**
Loss of life or personal injury	-	-	23	-	-	-	-	-	-	-	455	-	33	4	3	40	58	**616**
Money laundering	85	-	117	-	-	-	-	-	-	28	9	21	-	3	-	-	9	**272**
Murder	-	-	19	-	-	-	-	-	-	3	209	-	14	3	4	27	24	**303**

Offences involving planning and organisation	1	-	13	-	-	-	-	-	-	-	134	-	-	-	-	7	18	**173**
Organised offences and/or criminal organisations	5	-	10	-	-	-	-	-	-	1	17	-	-	-	-	-	-	**33**
People smuggling and related	-	-	9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**9**
Serious damage to property and/or serious arson	-	-	4	-	-	-	-	-	1	-	40	-	-	2	-	6	11	**64**
Serious drug offences and/or trafficking	197	-	464	-	-	-	-	3	17	121	816	4	202	20	6	50	196	**2,096**
Serious fraud	3	-	23	1	1	-	-	-	-	4	57	13	1	1	-	3	1	**108**
Serious loss of revenue	20	-	29	-	-	-	-	-	-	-	2	-	-	2	-	3	-	**56**
Special ACC investigations	44	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**44**
Telecommunications offences	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**0**
Terrorism financing offences	5	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**7**
Terrorism offences	-	-	113	-	-	-	-	-	-	-	4	-	-	-	-	1	-	**118**
TOTAL	**376**	**5**	**882**	**42**	**24**	**7**	**23**	**14**	**18**	**157**	**1,860**	**47**	**256**	**40**	**13**	**143**	**323**	**4,230**