Report of the Review of the Use of Surveillance Devices in Prisons

Tasmania 2024.

Damian Bugg AM KC

Contents

Summary of Review Findings and Recommendations.

My Review considered in detail the provisions of the Police Powers (Surveillance Devices) Act 2006, the decisions of Justice Brett in STATE of TASMANIA v. THOMPSON [2022] TASSC 53 (28 March 2022) and TASMANIA v. THOMPSON (No 2) TASSC 55 (28 July 2022), and all 19 surveillance device warrants issued between 1 January 2012 to 1 January 2024 authorising the installation of surveillance devices in a prison in Tasmania.

Early in the process of the Review, which I explain in the Report, I sought comment from and had discussions with people who had expressed concerns about the matters under Review or the breadth of the Terms of Reference of the Review, and people who were, from their professional positions, likely to have an interest in the matters I would be examining. I did not invite submissions by public advertisement, the issues I had to consider were well defined and scoped within the Terms of Reference.

I concluded that there were minor issues in the process of applications for warrants, not affecting validity, which could be improved and that an internal review, undertaken immediately after the decision of Justice Brett, handed down on 28 July 2022 (above) had already introduced changes which addressed many of those issues.

4 of the 19 warrants I examined were invalid on their face. One was the warrant considered in Thompson (above) and the other three were issued during the investigation of the same matter, containing an identical flaw through reliance on the form used, as a precedent, in the first warrant application in the investigation. I examined all four matters very carefully and the outcomes enabled me to conclude that no evidence or recording obtained through those warrants was produced in contested court proceedings other than in the Thompson trial, where the evidence was not admitted.

I am satisfied that the only operation of a surveillance device in a professional meeting room during a time when the target of the investigation for which a warrant issued was not meeting in that room was the matter considered by Justice Brett in Thompson. Because of concerns expressed to me about that episode of recording I interviewed all 5 officers who were authorised to operate or were capable of operating those two recording devices during the period they were operating. I also interviewed 7 of the 8 officers working in the operations room to which one of the devices was capable of transmitting. I am satisfied, and have met and personally assured all but one of the people who expressed concern to me, that no recording of any conversation external to the matter under investigation was monitored or downloaded from those devices and on their retrieval they were ‘wiped’ without play back.

I found that there were four warrants involving periods of continuous recording, one which I have commented on (above) and three others. Those three warrants concerned contact visit areas, not professional meeting rooms and I have concluded that they do not raise similar concerns as those dealt with in Thompson.

The Recommendations which I make in the report are, to an extent, already addressed by the reforms introduced following the internal review by Tasmania Police in 2022. I comment on that in the recommendation section for TOR 5 commencing on page 65.

RECOMMENDATIONS.

a. Assistance from Legal Services Division in preparation of warrant application documents for lodging with the court. The task of preparing an application, affidavit and draft warrant is not simple and assistance will help deal with some minor issues which I noted. My proposed recommendation has already been addressed through the internal review.
b. Better communication between investigator and Technical Support officer(s) in the preparation of documents for submission to the court.
c. I found issues with the draft warrant, submitted to the magistrate as a draft, containing superfluous clauses which could be deleted and closer attention needs to be given to the 'conditions' clauses.
d. Care to be taken when considering the alternatives of specified premises and specified persons warrants or a combination of the two.
e. The duration of warrants, a maximum of 90 days, needs to be considered in every application. Sometimes a shorter defined term may be appropriate, but shorter terms compel retrieval steps which may not be possible with covert operations.
f. Care with checklist of legal compliance issues.
g. Reliance on precedents must be exercised with care.
h. Changes in circumstances which require operational changes to the surveillance task must be reviewed with advice and consideration given to an application for variation of the terms of the initial authorisation in the warrant.
i. Section 29 reports should be completed, dated and signed by the issuing officer and checked before filing under section 37(f) of the Act.
j. A refocussed training model for serving officers and trainees. (This issue is being addressed as part of the internal review recommendations and the training model will be expanded because of the discovery of the incomplete inspections. (further detail in Safeguards section, to follow.)
k. I comment on legal professional privilege, as required in TOR 6 on page 70.

(iii)

SAFEGUARDS.

I consider the question of safeguards in the Report because the invalidity found in the Thompson matter, which was an 'error' repeated through the use, as a precedent, of a form containing the same error.

The first safeguard is the requirement that the formal application for a surveillance device warrant must be supported by an affidavit setting out the grounds on which the warrant is sought, thus requiring the applicant officer to swear the contents of the document to be true and correct. (s 9(3)(b)).

The second safeguard is the statutory requirement that an application for a warrant must be determined by either the Supreme Court or a magistrate and quite detailed requirements within the Act must be satisfied.

The third safeguard is the requirement under s 29 of the Act that a report, the form for which I will examine in the Report, must be completed and seen by the issuing Judge or magistrate and then retained by the chief officer of the law enforcement agency.

The fourth safeguard is provided through the record inspection activity of the 'inspection entity,' appointed pursuant to s 40 of the Act. In Tasmania the inspection entity is the Ombudsman and I conclude in the Report at page 72 that the Ombudsman has not, since the Act commenced in 2009, been undertaking inspections to 'determine the extent of compliance with the Act by the agency and law enforcement officers of the agency' as required by s 41 of the Act. I examine this issue, provide a suggested short term solution, and report on the results.

I conclude this section, and my Report by considering whether other safeguards and measures are needed, such as a Public Interest Monitor (PIM), which is provided for in Queensland and Victoria, recommending that, at this stage, such a step is not necessary.

I also consider in the Report the question of merger of the Act with the other Devices (Listening) Act in Tasmania and the breadth of the terms of reference of this Review, recommending that there are reasons for not undertaking the former (p. 10) and that for reasons related to the proposed solution to the lack of inspections under s 41 the Review has, in effect, achieved that broadening, scrutiny of other than 'in prison' surveillance device warrants.

Background Of the Review.

In March 2022 in the Supreme Court of Tasmania Jeffrey Ian Thompson was being tried on indictment for two counts of perverting justice. The admissibility of evidence which the prosecution sought to adduce in the trial was challenged on Voir Dire. One of the grounds of objection was that the evidence, obtained through use of two surveillance devices installed and operated under the purported authorisation of a warrant issued by a Magistrate under the Police Powers (Surveillance Devices) Act 2006 (Tas) ('the Act"), was unlawfully obtained because the warrant was invalid on its face. Justice Brett, the trial Judge, upheld the objection, ruling that the warrant was invalid because it did not comply with a requirement under the Act to specify the alleged offence in respect of which the warrant was issued. The warrant, on its face, referred to the crime of "conspiracy contrary to section 297(2)". There is no crime of conspiracy under section 297(2) of the Criminal Code.

The 'second step' in the Court's consideration of the question of admissibility was for Justice Brett to determine, under section 138 of the Evidence Act, whether the evidence, although obtained in contravention of the Act, should be admitted in the exercise of his discretion, guided by the provisions of that section.

The evidence which the prosecution had sought to adduce was the visual and audio recordings of conversations between the accused Thompson and a prisoner at Risdon Prison, Stephen Gleeson, which were recorded on two surveillance devices operating in a professional meeting room in Risdon Prison where the two parties met on June 16th 2017. Evidence given on the voir dire disclosed that the surveillance devices, installed shortly before the June 16th meeting, continued to operate and record in that meeting room after the meeting between Thompson and Gleeson and until they were removed on August 17 2017. One of those devices was capable, with technical knowhow, of being monitored remotely, by transmission to another location. In this case the transmission was made to the operations room at Police Headquarters for the detectives investigating the alleged conspiracy.

His Honour declined to admit the evidence finding that the Magistrate who issued the surveillance device warrant, while not deliberately misled by the police officer seeking the warrant, was not made aware that the devices installed pursuant to the warrant would continue to record for almost two months after the meeting between Thompson and Gleeson. His Honour found that there was, through this ongoing recording, a 'real risk to privacy arising from the near certainty that unrelated private and privileged conversations would be recorded and were capable of being monitored during the life of the warrant' and therefore 'greater detail should have been provided to and considered by the magistrate before issuing the warrant.'

This ruling resulted in the discontinuance of the prosecution of Thompson. His co accused, Gleeson, had pleaded guilty to the charge in March 2018 and was sentenced to a term of imprisonment of twelve months. Tasmania Police undertook an internal review of procedures following the ruling and the Commissioner of Police also committed to this Independent Review. I will be commenting on the outcome of that internal Review in my report.

The Terms of Reference for the Review were settled and tabled in both Houses of Parliament on 29 September 2022.

The commencement of the Review was delayed because of the need to amend the provisions of the Act which, under section 33, prohibit the communication or publication of 'protected information'. Under section 32 of the Act 'protected information' includes any information relating to an application for, issue of, existence of or expiry of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation. Clearly a Review with terms of reference requiring communication or publication of protected information to or by the reviewer may breach section 33 and therefore the conduct of the Review and reporting had to be exempted from the prohibitions in section 33.

The necessary amendments to the Act were passed by Parliament on 21 September 2023. I was appointed to undertake the Review in October 2023 and commenced backgrounding and interviewing in late October/early November 2023.

Terms of Reference and Scope of the Independent Review

The Terms of Reference document, tabled in Parliament, commences with a Background/Context outline which I will not repeat. The complete document is an attachment 'A' to this Report. The Objective and Scope of the Review follow a brief Definitions section.

Objective.

The Independent Review will involve consideration of all surveillance device warrants issued to Tasmania Police officers since 1 January 2012 which authorised the instillation and use of a surveillance device in a prison. It will consider the adequacy of information included in the applications for those warrants and compliance with any conditions or limitations imposed on the warrants. The reviewer will be requested to identify any improvements which could be made in applications for the issue of surveillance device warrants or the execution of such warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought and to prevent access to, or retention of, any such conversations.

Scope.

The Review will:

1. Review all surveillance device warrants issued to Tasmania Police officers since 1 January to the present day which authorised the installation and use of a surveillance device in a prison.
2. Consider the adequacy of the information provided to issuing officers in applications for the use of surveillance device warrants within the scope of the Review in relation to:
    i. the risk of the use of the surveillance device resulting in the capture of private conversations unrelated to the investigation in respect of which the warrant was sought;
    ii. proposed measures to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.
3. Consider the adequacy of any conditions or limitations imposed by issuing officers on surveillance device warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.
4. Consider compliance by Tasmania Police with any conditions or limitations referred to in paragraph 3 and the adequacy of any measures taken by Tasmania Police of its own volition to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.
5. Identify any improvements which could be made in applications for the issue of surveillance device warrants or the execution of such warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought and to prevent access to, or retention of, any such conversations.
6. Consider whether any specific measures are required to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought which may be subject to legal professional privilege and prevent access to, or retention of, any such conversations.

Approach.

The review will be undertaken independently of Tasmania Police.

Tasmania Police is fully supportive of this review and will assist the reviewer with any requests to access staff and records.

Outline of the Approach to and Conduct of the Review.

The Scope of the Review, under the Terms of Reference, limits the Review to a consideration of the Applications for, Issuing and Execution of and Reporting on surveillance device warrants which authorised the installation and use of surveillance devices in a prison, (defined), from 1 January 2012 to the present day. I will comment further on the Scope of the Review later in my report.

COMMENCEMENT AND CONFIDENTIALITY ASSURANCE

There were unavoidable delays in commencing the Review. The amendments to the Act which I have mentioned were not finalised until September 2023, by which time the person originally tasked with undertaking the Review was committed with other duties until April 2024. When Commissioner Adams, the Commissioner of Police, approached me to discuss my availability to undertake the Review she made me aware of the time already taken in preparing a way for the Review.

I familiarised myself with the Terms of Reference/Scope document, relevant decisions of Justice Brett and steps already taken by Tasmania Police, in the internal review, to address issues identified in Justice Brett's decisions, I met with Commissioner Adams and Senior Officers of Tasmania Police to outline my approach to the Review and the level of cooperation and support I would require to undertake the Review. I also explained the approach I proposed to take in my report in dealing with 'protected information,' issues and discussions with, and identities of, officers from whom I would be seeking answers and information on surveillance device technology and methodologies, for which there are certain statutory protections (s. 34 of the Act). Those statutory protections relate to evidence in 'proceedings' which of course my Review and reporting are not. However, I took the view from the outset that 'surveillance device technology and methodologies' ought not, in the public interest, be disclosed in detail or publicised by me, and I gave such an assurance during that first meeting.

Clearly a thorough examination of the issues within the Review scope would require an understanding of surveillance device technology and the methodology of the use of such devices, but it did not necessarily follow that my reporting of those issues would require disclosure of such matters. If that position changed as the Review progressed then I would, of course, carefully re consider that initial assurance. Having concluded my interviews with many of the Technical Surveillance Services ("TSS") officers whose duties over the review period included the 'installation, use and retrieval of surveillance devices and dealing with surveillance device technology' (section 34), I have concluded that I am able to report on my findings and recommendations without disclosing identities, technology and methodology.

Those assurances, given to the Commissioner and Senior Officers, have also enabled TSS officers operating in this area to more freely discuss matters with me, which in turn has given me a better understanding of why certain approaches have been taken and procedures followed.

PROTECTED INFORMATION AND THE EXEMPTION FROM THE PROHIBITION IN SECTION 33 OF THE ACT.

Under s. 32 of the Act 'protected information' means :-

(a) "any information obtained from the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

any information relating to :-

(i) an application for, issue of, existence of or expiry of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or
(ii) an application for approval of powers exercised under an emergency authorisation; or
(iii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation; or

(b) any information obtained by the use of a personal camera, in accordance with section 44A, by a police officer."

The highlighting in yellow, as explained in the next section, covers all matters within the definition of protected information which fall for consideration in all the warrants and matters the Review will cover and through which the amendment to the Act will provide me with the assurance of an exemption. That exemption inserted subsection 3A in s. 33 of the Act, provides that :-

"(3A) Subsections (1) and (2) (The penalty provisions for communicating or publishing protected information) do not apply to :-

(a) the use or communication, of protected information, for the purposes of conducting a review into the use of surveillance devices in prisons, within the meaning of the Corrections

Act 1997, that is undertaken in accordance with the terms of reference tabled in both Houses of Parliament on 29 September 2022, as amended from time to time; or

(b) the use of protected information in a report, in relation to the review referred to in paragraph (a), that is made by the person who conducted the review and the publication of the report; or
(c) the use, communication, or publication, by the Minister, of protected information contained in a report referred to in paragraph (b)-

if the use, communication, or publication is on accordance with any conditions imposed in respect of the terms of reference referred to in paragraph (a)."

I have included the full text of the amendment in this report as I will return to consider it in detail when I examine the Scope of the Review and an issue concerning oversight.

Since that initial meeting I have communicated with Commissioner Adams and Assistant Commissioner Blackwood on occasions to inform them of the progress of the Review and a likely reporting date and to also seek their consideration of a suggestion concerning the breadth of the terms of reference. From the outset I was assured of and have received the full cooperation of Tasmania Police, ably assisted by Senior Legal Officer Rebecca Munnings of the Legal Services Division, Tasmania Police, who has arranged meetings with more than 30 officers, during December and January, when requested and provided documentation and access to internal records to me when called for. Her assistance in providing details of reviewed procedures following the earlier internal review, later record inspection and proposed training programme have also been very helpful.

I have also been assisted in my task by the ready cooperation of a number of people who freely gave of their valuable time and professional expertise when contacted. I will formally acknowledge that assistance when considering relevant issues in my Report.

THE SCOPE OF THE REVIEW

I was, initially, provided with files relevant to 17 surveillance device warrants issued during the period covered within the Scope of the Review. Those files consisted of copies of original documents relevant to the application for and issue and execution of Surveillance Device Warrants for installation of a surveillance device in a prison in Tasmania. Each file contained the application for the warrant, affidavit in support of the application, the warrant issued together with any documents relevant to an application for an extension of the warrant and the report to the Magistrate under s. 29 of the Act. Initially I read the 17 files to understand the procedures followed, the nature and extent of the evidence provided by affidavit and the form and content of the warrants issued and the outcomes of the execution of the warrants from the s. 29 reports.

Under s. 11(2)(e) of the Act the issuing officer (the Magistrate) 'must' have regard to 'any previous warrant sought or issued under this Division….in connection with the same offence.' On reading the affidavits lodged in support of applications for two of the 17 warrants I noted that the officer applying for the warrant provided information of a previous surveillance device warrant issued in connection with the same offence which was not in the bundle of files. I was informed that in each of those two warrants the proposed meeting, for which the surveillance device warrant was sought, did not take place, and there was no recording from the surveillance device. As the surveillance device warrants had, in any event, been "issued" to Tasmania Police officers they had to be included in the Review.

The additional files were provided and the Review was expanded to involve consideration of a total of 19 surveillance device warrants issued to Tasmania Police officers during the relevant period.

All 19 warrants were issued by a magistrate, and were issued in response to an application, supported by an affidavit sworn by a police officer ('a law enforcement officer', s. 3 of the Act). As a consequence the Review will not consider any application to or process involving the Supreme Court, which may issue any warrant under the Act, including warrants authorising the use of a surveillance device warrant outside Tasmania. (magistrates do not have the power to issue extra jurisdictional warrants). Likewise, because none of the warrants issued was applied for remotely (s. 10) nor were any applications made urgently, before an affidavit could be prepared and sworn (s. 9(4) and (5)) I will not include in this Review any consideration of the procedures applying to such applications. For this reason, in the previous section, I highlighted in yellow the portions of the definition of "protected information" in s. 32 which relate to those procedures in the 19 warrants covered by the Review. Supporting evidence and consideration of it by issuing officers, which would be relevant to any of the procedures now not covered will, in an evidentiary sense, be covered when I consider sufficiency of affidavit evidence later in the Review.

I have interviewed every police officer who applied for and swore an affidavit in support of the 19 warrant applications during the relevant period. I have taken in to account the issues or concerns raised by Justice Brett in his voir dire decisions in the trial of Jeffrey Ian Thompson (State of Tasmania v. Thompson (2022) TASSC 53 (28 March 2022) and State of Tasmania v. Thompson (2022) TASSC 55 (28 July 2022)) when examining the 19 affidavits accompanying the warrant applications, the warrants and s. 29 reports and when interviewing the officers.

I will consider the files for each of the 19 warrants in light of these decisions, after first considering the provisions of the Act concerning applications for, execution of and reporting on surveillance device warrants and the procedures outlined to me by the officers interviewed.

The Terms of Reference and Scope document also reflect the concerns raised by Justice Brett in his decisions and set the parameters for the exemption for the Review in the amendment to the Act, defining the breadth of the matters and issues I can consider. I will therefore examine in detail the surveillance device element of the investigation of the suspected conspiracy to pervert justice

involving Jeffrey Thompson and Stephen Gleeson. Justice Brett's decisions will also inform my Review of the other 18 warrants covered in the Review. The warrant issued in the Thompson/Gleeson investigation is one of the 19 warrants included in my Review.

I have interviewed 7 detectives involved in the investigation of Thompson and Gleeson and all 5 Technical Support officers working in the Technical Support Branch at the time of that investigation. The information from those interviews will also inform my examination of the 19 matters and the approach taken.

Surveillance Device Warrants in Tasmania

1. The Police Powers (Surveillance Devices) Act 2006

People who participate in activities in public places cannot expect an absolute protection of privacy, they may be photographed, listened to and watched and while privacy is protected to an extent by Parliament and the courts, 'Tasmania does not have legislation granting a general right to privacy and there are few limitations on the use of surveillance devices in or from public places.' (extract from the Second Reading Speech "Police Powers (Surveillance Devices) Bill 2006 (No.34) Legislative Council Tasmania, 21 November 2006).

In 1991 the Tasmanian Parliament had passed the Listening Devices Act which prohibited a person from using or causing or permitting to be used, a listening device to record or listen to a private conversation to which the person is not a party or to record a private conversation to which the person is a party (see s. 5(1)). Under that act a 'listening device is defined as any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with it taking place', and a private conversation 'means any words spoken by one person to another person or to other persons in circumstances that may reasonably be taken to indicate that any of those persons desires the words to be listened to only by themselves or by themselves and by some other person who has the consent, express or implied, of all those persons to do so'. The prohibition is clearly not limited to conversations taking place on private premises.

The Listening Devices Act prohibition in s. 5 (above) does not apply to the' use of a listening device pursuant to a warrant granted under Part 4 of the Act', and uses of listening devices pursuant to authorisations under other legislation, including, after it commenced, the Police Powers (Surveillance Devices) Act 2006 (the Act). And to emphasise the seriousness of the prohibition, an offence against the provisions of the act, for which there is not a specific penalty, may on conviction incur a maximum sentence of 2 years imprisonment and/or a fine of $7,600. (s. 12 (a))

I include this reference to the Listening Devices Act in the Review for two reasons:-

(i) It precedes the Act by 15 years but contains a defined process and an example of the safeguards Parliament will require when providing law enforcement authorities with powers to use covert surveillance in the investigation of suspected wrongdoing, and

(ii) It's legislative history provides an explanation for the Tasmanian Parliament choosing, in 2006, not to merge the newer surveillance devices legislation with the Listening Devices Act (an issue I first considered myself when reading the two acts and later when raised with me by three people with whom I spoke as part of this Review) The warrants, creating the exemptions from the prohibition in s. 5 of the Listening Devices Act are, under Part 4 of that Act, obtained by a police officer of or above the rank of Sergeant from a magistrate in circumstances and following a process which is not dissimilar to the processes which must be followed under the Police Powers (Surveillance Devices) Act 2006 ('The Act").

The differences of note between the two acts appeared capable of simplification through merger:

(a) The rank of police officer applying for the warrant was different (Sergeant for one and any officer for a surveillance device warrant)
(b) The Australian Crime Commission was included in the later Act.
(c) Only a Supreme Court Judge could issue a cross jurisdictional warrant in the surveillance Act
(d) The offence under investigation for a listening device had to be indictable and for a surveillance device warrant an offence punishable by a maximum term of imprisonment of 3 years or more.

The cross jurisdictional issues and, in my view, the continuing separation of the two acts are explained in the following passages of the Surveillance Devices Bill Second Reading speech referred to on page 8. I will include these passages because they explain to those anticipating a recommendation for a merger of Tasmanian surveillance and listening device legislation why I have chosen not to grasp that nettle. I do not think it is necessary.

SECOND READING SPEECH, Police Powers(Surveillance Devices) Bill. Legislative Council.21/11/2006.

"The bill will allow officers of Tasmania Police and the Australian Crime Commission" (established in 2002)"to use a greater range of surveillance devices to investigate Tasmanian offences. The Commonwealth's Surveillance Devices Act 2004 already confers on a State or Territory police force and on the ACC a range of similar powers that can be used in investigating Commonwealth offences. Less intrusive surveillance may be carried out without a warrant and this will continue to be the case. Police here and in all other jurisdictions have engaged in certain types of surveillance as part of their investigation on offences and crimes without a warrant. This is routine police work and it must not be subject to unnecessary restrictions which would destroy police effectiveness.

“Under the bill and the Commonwealth Act as well, a warrant is required when the use of a surveillance device is otherwise unlawful. The underlying policy is to prevent the unwarranted intrusion in to the privacy of individuals through the use of surveillance devices.

“Tasmania does not have legislation granting a general right to privacy and there are few limitations on the use surveillance devices in or from public places. Watching or photographing in and from public or private places does not usually involve any unlawfulness but entry onto property without consent or interfering with premises, computers or vehicles to facilitate surveillance activities could involve unlawful activity including interference with or damage to private property. So legislation is necessary to ensure that this can be undertaken with appropriate safeguards.

“The only significant piece of Tasmanian legislation relevant to this matter at the moment is the Listening Devices Act 1991 which makes it an offence to use a device to listen to and/or record private conversations without the knowledge or consent of the parties to the conversation or, if the person doing the recording was a party, without the consent of the other party to the private conversation.

And later “This bill, in line with the national model bill arising from the joint working party report on cross-border investigative powers, provides that a warrant will be able to be sought for the investigation of offences which carry a maximum penalty of at least three years’ imprisonment. This provides a slightly wider range of offences than the Listening Devices Act where warrants are granted in respect of indictable offences. The number of offences attracting at least three year terms of imprisonment which are not indictable offences are relatively few but importantly they do include some drug offences which carry penalties of four years’ imprisonment.

“The bill will provide for a warrant to be issued for the installation and use of data surveillance devices, listening devices, optical surveillance devices and tracking devices. Generally, as with the listening devices currently, a warrant will be obtained from a magistrate. However to ensure alignment with the national model and to facilitate mutual acceptance and recognition of the use of powers when an investigation will be undertaken in another jurisdiction, the warrant will need to be issued by a judge of the Supreme Court.”

The speech then moved to consider safeguards within the bill, but I will be considering those in detail within this report. The safeguards referred to were passed without any relevant amendment.

I am satisfied that those passages provide a sufficient basis for me to conclude that the Listening Devices Act 1991 and the Police Powers (Surveillance Devices) Act 2006 should remain separate, certainly in so far as the issues raised in this Review are concerned.

The Act is based on a national model bill, linked with the Commonwealth Act of 2004, provides for cross jurisdictional warrants to be issued by judges and covers a wider range of offences than covered by the Listening Devices Act.

LEGISLATIVE REQUIREMENTS and PROCEDURES COVERED BY THIS REVIEW.

All 19 warrants I have considered were issued by a magistrate following an application lodged by an investigating police officer with the magistrates court either in Launceston or Hobart. As noted earlier, none of the 19 applications were remote or urgent, for which there is a slightly different procedure, nor did they concern authorisation of the use of a surveillance device outside Tasmania. (Extra jurisdictional warrants are issued by the Supreme Court). As indicated with yellow highlighting on page 5, I will confine the extent of my consideration of the process of application accordingly, but the evidentiary issues will be the same for the excluded procedures, in terms of those clauses in the Scope of the Review, which are relevant to the provision of evidence or information to the issuing authority.

‘ surveillance device’ under the Act means :-

(a) a data surveillance device, a listening device, an optical surveillance device or a tracking device, or
(b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a); or
(c) a device of a kind prescribed by the regulations.

Two types of warrant may be issued under Part 2 of the Act, a surveillance device warrant or a retrieval warrant (s. 7(1)) and a warrant may be issued in respect of one or more kinds of surveillance devices (s. 7(2)).

There are no retrieval warrants in the 19 matters I am considering and I will not therefore cover any aspect of the processes for retrieval. In any event, every surveillance device warrant also authorises the retrieval of the device installed pursuant to that warrant. (s. 13(3)(a)), permitting the applicant for the warrant to arrange for the retrieval of the device after installation. And any extension of such a warrant will achieve the same outcome.

The Supreme Court may issue any warrant under Part 2 of the Act whereas a Magistrate may issue a surveillance device warrant ‘other than one which authorises the use of a surveillance device outside Tasmania’.

APPLICATIONS FOR A SURVEILLANCE DEVICE WARRANT. (SECTION 9 OF THE ACT).

The threshold for an application for a warrant to be made is that the offence under investigation must be a ‘relevant offence,’ defined as an offence punishable by a maximum term of imprisonment of 3 years or more. This limitation emphasises the seriousness of the alleged criminal conduct which will trigger the privacy intrusion permitted by a warrant issued under the Act.

A law enforcement officer or another person on his or her behalf may apply for a surveillance device warrant under s. 9 of the Act. “Law enforcement officer” is defined under the Act to mean a police officer and in relation to the Australian Crime Commission, a member of staff of the Australian Crime Commission, and includes a person who is seconded to a law enforcement agency, including (but not limited to) a member of the police force or police service and a police officer (however described) of another jurisdiction. (s. 3(1))

Under the Act a law enforcement officer may apply for a surveillance device warrant provided the following circumstances exist and steps are followed:-

1. If that officer on reasonable grounds suspects or believes that
   (a) a relevant offence has been, is being, is about to be or is likely to be committed; and
   (b) an investigation in to that offence is being, will be or is likely to be conducted in this jurisdiction and
   (c) the use of a surveillance device is or will be necessary in the course of that investigation for the purpose of enabling evidence or information to be obtained of the commission of the relevant offence or the identity or location of the offender. (s. 9 (1) (a) and (b) and (c).

2. The application may be made to the Supreme Court or a magistrate. (s. 9(2)(a) and (b)
3. the Application must specify (a) the name of the applicant and (b) the nature and (c) the duration of the warrant including (c) the kind of surveillance device sought to be authorised. (s. 9(3)(a) (i) and (ii)
4. The application must be supported by an affidavit setting out the grounds on which the warrant is sought and the prescribed information (if any).

The application must be heard by either the judge or magistrate in the absence of anyone other than (a) the applicant, (b) someone the judge or magistrate permits to be present, (c) and an Australian legal practitioner representing anyone mentioned in (a) or (b), and the application must be heard in the absence of the person proposed to be placed under surveillance or anyone likely to inform that person of the application and without that person being informed of the application (s. 9 (6) and (7)).

The hearing of an application for a surveillance device warrant under the Act, supported by an affidavit and heard ex parte, is therefore very dependant on the detail in the application and the content of the affidavit in support. While some indication as to the contents of the affidavit is given in the provisions of the Act outlined in the circumstances and steps above, further direction is obtained from s. 11 of the Act “Determining the application”, which provides:-

11(1) The Supreme Court or a magistrate may issue a surveillance device warrant if satisfied:-

(a) That there are reasonable grounds for the suspicion or belief founding the application for the warrant;

(2) in determining whether a surveillance device should be issued, the judge or magistrate must have regard to:-

(a) the nature and seriousness of the alleged offence in respect of which the warrant is sought; and

(b) the extent to which the privacy of any person is likely to be affected; and

(c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation: and

(d) the evidentiary or intelligence value of any information sought to be obtained; and

(e) any previous warrant sought or issued under this Division, a corresponding law (if known) or the Listening Devices Act 1991 in connection with the same offence.

The requirements both for an application and supporting affidavit call for an awareness of the investigation being undertaken and more generally the process of that investigation. The importance of this is further emphasised when the provisions of the Act concerning what a surveillance device warrant must contain and what the warrant authorises are placed in the same basket. I will continue this examination of the requirements of the Act to provide a better understanding of both the complexity of the warrant application process and the need for attention to detail by all persons concerned in this process.

While the hearing of the application and the issuing of a surveillance device warrant are conducted by a Judge or magistrate ex parte, the proceeding is not a judicial one but rather an administrative act “exercised judicially.” The commitment of investigative resources and the approval of covert means involving surveillance devices used under the authority of a warrant issued by a Judge or magistrate are now well settled but with an expectation both from Parliament and the courts that the evidence will be fairly weighed by the issuing magistrate or Judge in a proceeding where not all parties are represented.

" The issuing of a warrant can be described as a judicial act but not in the sense of an adjudication to determine the rights of the parties. Although judicial review is available to review the exercise of the power to issue a warrant, it is available whether the power be classified as judicial or administrative in nature. And although the duty to exercise the power to issue the warrant must be exercised judicially, that means only that the power must be exercised without bias and fairly weighing the competing considerations of privacy and private property on the one hand and law enforcement on the other" (Grollo v Palmer (1995) 184 CLR 348 at 361).

WHAT MUST A SURVEILLANCE DEVICE WARRANT CONTAIN.

S. 12 of the Act contains the following provisions

"12(1) A surveillance device warrant must:-

(a) state that the Supreme Court or magistrate is satisfied of the matters referred to in s. 11(1) and has had regard to the matters referred to in s. 11(2); (in other words must state that he or she is satisfied that there are reasonable grounds for the suspicion or belief on which the application is founded , and has had regard to the 5 matters in s. 11(2), see page 13). All of which draws attention to those requirements at the time of completing the details in the warrant.

(b) Specify:-
   - (i) the name of the applicant; and
   - (ii) the alleged offence in respect of which the warrant is issued; and
   - (iii) the date on which and the time at which the warrant is issued; and
   - (iv) the kind of surveillance device authorised to be used; and
   - (v) if the warrant authorises the use of a surveillance device on premises, the premises on which the use of the surveillance device is authorised or to which entry is authorised in relation to the use of a surveillance device on other premises; and
   - (vi) if the warrant authorises the use of a surveillance device in or on an object or class of objects, the object or class of objects in or on which the use of the surveillance device is authorised; and
   - (vii) if the warrant authorises the use of a surveillance device in respect of the conversations, activities and geographical location of a person, the name of the person (if known); and
   - (viii) if the warrant authorises the use of a surveillance device in a participating jurisdiction, the participating jurisdiction in which it may be used; and
     the period during which the warrant is in force, being a period not exceeding 90 days; and
   - (ix) the name of the law enforcement officer primarily responsible for executing the warrant; and

(x) any conditions subject to which premises may be entered, or a surveillance device may be used, under the warrant; and

(xi) the time within which a report in respect of the warrant must be made to the Supreme Court or the magistrate under section 29.

12 (2) In the case of a warrant referred to in subsection (1)(b)(vii), if the identity of the person is unknown, the warrant must state that fact.

(3) A warrant must be signed by the person issuing it and include their name."

The demands for a high level of detail in the application, and evidence contained in the affidavit are demonstrated by a simple addition of the compulsory content requirements for any warrant which are detailed in s. 12, approximately 20 items, all of which must be carefully considered. This in turn further demonstrates the amount of information which must be processed and confirmed within a warrant by any Judge or magistrate hearing an application for a surveillance device warrant under the Act.

WHAT A SURVEILLANCE DEVICE WARRANT AUTHORISES.

S. 13 of the Act provides that a surveillance device warrant may authorise any one or more of three uses for a surveillance device:-

13(1)(a) … on specified premises;

(b)….. on a specified object or class of objects;

(c)…..in respect of the conversations, activities or geographical location of a specified person or a person whose identity is unknown.

On page 11 the five kinds of surveillance device are listed, data surveillance device, a listening device, an optical surveillance device and a tracking device, or a device which is a combination of any two or more of those devices.

It is possible therefore that a warrant may, for example, authorise the use of a listening device on specified premises, an optical surveillance device on an object and an audio optical device in respect of conversations of a specified person or one who is unknown. The draft forms for an application for and the actual surveillance device warrant must therefore be capable of accommodating all these options.

A warrant authorising any of the three uses above also, by virtue of the provisions of s. 13, authorises the installation, use and maintenance of the device(s) specified on the premises, the object or class of objects, or the premises where the person is reasonably believed to be or likely to

be and the entry by force if necessary, onto the premises, or other specified premises etc for the purpose of installing, maintaining or using the device(s). (s. 13(2)).

There are additional authorisations specified in s. 13 which, for completeness I will detail.

13(3) Each surveillance warrant also authorises:-

(a) the retrieval of the surveillance device; and
(b) the installation, use, maintenance and retrieval of any enhancement equipment in relation to the surveillance device; and
(c) the temporary removal of an object from any place where it is situated for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment and the return of the object to the place or another appropriate place; and
(d) the breaking open of anything for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment; and
(e) the connection of the device or equipment to an electricity supply system and the use of electricity from that system to operate the surveillance device or enhancement equipment; and
(f) the connection of the surveillance device or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the device or equipment; and
(g) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for executing the warrant in the installation, use, maintenance or retrieval of the surveillance device or enhancement equipment.

(4) A surveillance device warrant may authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the installation, use, maintenance or retrieval of a surveillance device or enhancement equipment.

(5) A law enforcement officer may use a surveillance device under a warrant only if he or she is acting in the performance of his or her duty.

(6) This section applies to a warrant subject to any conditions specified in the warrant.

THE ROLES OF OFFICERS INVOLVED IN OBTAINING A WARRANT AND INSTALLING DEVICES

During the period covered by this review law enforcement officers seeking surveillance device warrants under the Act utilised templates which were available for both the Application and the Draft warrant which accompanied the Application. I attach (marked 'B' and 'B1') copies of those documents and will refer to them, and their use during the balance of this report. A template was also provided for the accompanying affidavit, a copy of which is not necessary. I will address affidavit issues specifically without the need to refer to the template.

I will outline the roles and responsibilities, during the period covered by this Review, of the police/law enforcement officers involved in the process of applying for a warrant to use a surveillance device. The installation of devices authorised to be installed under the warrant and the management of the use and retrieval and reporting on the use and retrieval of the device(s) will have a different focus. I will avoid specific reference to process and detail concerning the functioning of any device which may disclose technology or methodology relevant to surveillance device activities of the Technical Surveillance Services Division ("TSS") of the Tasmania Police Department. TSS is a technical service and support unit of Tasmania Police which is quite separate and independent from but a technical service for investigations undertaken by the Criminal Investigations Branches. TSS is not an investigative agency. That separation and independence will be highlighted in my consideration of the second third and fourth Terms of Reference. (page 3)

A. Criminal Investigation Branch (CIB) and Surveillance Device Warrants

Officers of the CIB undertaking an investigation which reaches a stage where the use of a surveillance device may provide further evidence or assistance with the investigation will be guided by this check list of questions and issues, taken from the Act, which provide an evidentiary basis to support an application for a surveillance device warrant.

(1) Does the officer who will apply for the warrant suspect or believe, on reasonable grounds, that
   (a) a 'relevant offence' (one punishable on conviction with a maximum term of imprisonment of three years or more) has been committed, is being committed, or is about to be or likely to be committed, and
   (b) an investigation into the offence is being, will be or is likely to be conducted in this jurisdiction, and
   (c) the use of a surveillance device in this jurisdiction is or will be necessary in the course of the investigation for the purpose of enabling evidence or information to be obtained of the commission of the relevant offence or the identity or location of the offender.

(2) Having considered those questions, the officer will also have to address the following matters:-

(i) are there alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation, and

(ii) what will the evidentiary or intelligence value of any information sought to be obtained be, and

(iii)can the warrant be justified considering the extent to which the privacy of any person is likely to be affected.

The factual basis for the resolution of these questions, supported by an outline of the evidence, facts or intelligence relied upon, will provide the bulk of the material for the investigator's affidavit in support of the application to the magistrate (or Judge) for the issue of a surveillance device warrant. The earlier inclusion of the relevant sections of the Act (pp13-15) provides details of the legislative source of the above check list. The first three are contained in s. 9 (1)(a)(b) and(c), the last three in s. 11(2)(b)(c) and (d).

When the review of the items in the checklist is complete and the investigators propose to utilise a surveillance device in the investigation an application is made, through command structure to the TSS to seek support. The TSS unit, as explained, is a covert technical services unit whose function is to supply technical advice and services to investigators. One such service is the installation and monitoring of surveillance devices under the authority of a warrant issued by a magistrate or Judge, and the capture (recording) of evidence/intelligence for the investigators.

B. Technical Support Services ("TSS")

While this is an over simplification of what occurs, it is sufficient for these purposes. The CIB application for TSS support will require an outline of what the investigators wish to observe or place under surveillance. Will it be optical, audio or tracking, or any combination, what conduct/activity involving whom, where and when? The TSS officer(s) will then assess/scope the task and on the determination of that assessment indicate whether the task is achievable.

Covert surveillance operations, understandably, involve quite different considerations, resources, technical services and manpower from task to task. A covert surveillance operation in a home, public open space, shop, shopping mall, prisons and custodial premises will each require a differing approach, also influenced by the purpose of the surveillance, to gather evidence, record conversations, movement of people, vehicles and goods.

The TSS assessment of these issues will inform the nature of the task and the technical resources necessary. If, in the technicians' opinion the task is achievable, or if deemed achievable, the application for TSS support for the investigation will be approved, however the level of information provided to the investigators will be limited. For security reasons there is virtually no information provided to detectives about the equipment, its location, technical capabilities and functioning and method of recording. There are very good reasons for this level of secrecy and security between divisions. Covert services provided by TSS, particularly those involving highly sophisticated devices and technology are just that, covert.

TSS policy requires officers assigned to and working within it to sign confidentiality agreements. These agreements require officers to protect from disclosure information concerning the technology, capability, methodology and use of surveillance, recording and enhancement equipment used by or available to this service. TSS officers are protective of this intelligence and will not disclose details to investigators or other officers. Jealously guarded and protected, this policy does sometimes frustrate investigators. I interviewed 6 TSS officers, in all cases their answers were the same, covert capacity and effectiveness would be at risk of compromise if there was any disclosure of information leading to an awareness of the technology capabilities and methodology of the TSS.

One aspect of this policy which I had not considered until I spoke with TSS officers, but which is borne out in the passages of the Second Reading Speech for the Police Powers (surveillance Devices) Bill is the co-operative arrangements between other Federal, State and Territory Surveillance support agencies. The exchange of information, facilities and equipment between these agencies would be at serious risk of compromise if loosely managed and functioning technical support services existed in any part of that network. The integrity of the protection of their 'intelligence' is only as strong as the practises of the weakest link. This policy, in an investigation will become evident when I consider the Thompson decisions.

The approval of TSS officers for a particular surveillance operation in support of an investigation will be conveyed to the investigator and then steps will be taken to apply for the surveillance device warrant. The applications for all 19 warrants I have reviewed followed such procedure, where the Application template (page 16) and the accompanying affidavit were lodged with the Magistrates Court together with the draft warrant (page 16).

PREPARATION AND LODGEMENT OF THE WARRANT APPLICATION.

The provisions of the Act dealing with applications, s. 9, have been set out previously and key triggers mentioned. The template in use during the period covered by this Review

and attached to this Report ('B') is appropriate and in a form which accommodates the requirements of s. 9(3) of the Act:-

(3) An application-

(a) must specify-

(i) the name of the applicant; and

(ii) the nature and duration of the warrant sought, including the kind of surveillance device sought to be authorised; and

(b)subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought and the prescribed information (if any)

There are three kinds of warrant specified in s. 13. A 'specified premises' warrant, a 'specified object' warrant and a 'specified person' warrant. (see s. 13 (1)) and, as mentioned, there are 5 different devices, data, listening, optical and tracking, or in combination.

The Application template makes provision for all these options in the three divisions of paragraph 3 of the template.

Paragraph 4 of the template provides for the term for which the warrant is sought which, under s. 12 (1)(b)(ix), must not exceed 90 days.

The Act permits an application for and any issued warrant to be in "extremely broad terms" (see Brett J., State of Tasmania v. Jeffrey Ian Thompson 28 March 2022 p2) His Honour there referring to paragraph 6 of the warrant under consideration, which is based on the template attached. I will have more to say about the permitted breadth of warrants after I consider the content of the applications for the 19 warrants under review one of which is the warrant which Justice Brett considered in the Thompson case.

The affidavit accompanying the application for the warrant, usually sworn by the officer applying for the warrant, must contain evidence which will substantiate the issues relevant to the Magistrates consideration of the application and completion of the warrant.

AFFIDAVIT IN SUPPORT OF THE APPLICATION FOR A WARRANT.

The affidavit must contain evidence and information which will enable the issuing magistrate to make a determination to issue the warrant and approve the terms and conditions of the warrant. That information and evidence (grounds) will be contained within the affidavit by

providing the following :-

(a) the deponent's rank and qualification as a 'law enforcement officer'
(b) what the application is for, a premises, object or person/conversation warrant
(c) identifying the relevant offence
(d) detail of the investigation which will include the basis upon which the application is founded under s. 9 (the commission of the relevant offence, the investigation and the stage it has reached and the necessity for the use of the surveillance device.)

The information and evidence provided in (a)-(d) will enable the magistrate to either be satisfied or not the "there are reasonable grounds for the suspicion or belief founding the application for the warrant" (s. 11(1)(a)) and proceed to determine whether the warrant should be issued.

The affidavit must also provide the magistrate with evidence or information in support of the following issues, of which the magistrate must have regard (s. 11(2) of the Act):-

(e)the nature and seriousness of the alleged offence in respect of which the warrant is sought, and

(f)the extent to which the privacy of any person is likely to be affected: and

(g)the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation; and

(h)the evidentiary or intelligence value of any information sought to be obtained; and

(i)any previous warrant sought or issued under this Division, a corresponding law (if known) or the Listening Devices Act 1991 in connection with the same offence.

The requirement that the application be supported by an affidavit containing the above information, of necessity, requires the deponent to be an officer who is familiar with and involved in the investigation. The requirement in (f) extends the knowledge requirement to an understanding of the covert surveillance device proposal, and that will always be limited because of the confidentiality requirements between investigators and TSS officers. This was also a matter of concern for Justice Brett in the Thompson case.

THE DRAFT WARRANT AND CONTENTS.

The requirements of the Act for the contents of a surveillance device warrant, (s. 12), are set out on pages 14 and 15, the template for the draft warrant which accompanies the application and affidavit, when lodged with the court, is available in the form which is attachment (B1). That document endeavours to simplify the tasks of the applicant and the magistrate or Judge who hears the application in settling the terms of the warrant.

The process of lodging this document, in draft form with the Application and affidavit in support, and the issuing of a warrant by the magistrate I found to be a problematic part of the process which was being followed during the period under review.

I have used the term 'draft warrant' for the document which is presented to the magistrate with the application and supporting affidavit because that is what it is. Many of the officers who were applicants for warrants in the 19 I have examined indicated to me when I interviewed them that their expectation from the process was that the magistrate would settle the final terms and conditions of the warrant, if one was to issue, and therefore there were gaps or options in the draft warrant which they presented. In few instances the magistrate required a specific condition to be included in the draft or the application process delayed for amendment. In other instances it appeared to me that the magistrate had regarded the draft warrant as containing the terms and conditions of the warrant which the applicant law enforcement officer was seeking and little or no change was made to the draft.

I did not interview any of the magistrates who were involved in issuing the 19 warrants I examined. I did not have the authority to do that and I did not feel that my terms of reference extended that far.

The Act is silent on the issue but I am in no doubt that the responsibility for providing a warrant in draft form with the Application and affidavit rests with the applicant law enforcement officer. I have previously drawn attention to the nature of the role which the magistrate is performing when determining whether to issue a warrant. The magistrate is performing an administrative role while acting judicially, in the sense of acting without bias and fairly taking in to account the competing interests of privacy and private property on the one hand and law enforcement on the other (Grollo v. Palmer. supra).

The issue for which there is no answer in the Act is the extent to which the applicant should attempt to complete the warrant, which, if overly detailed, may be interpreted as an attempt to pre-empt matters which fall to the discretion of the magistrate. On the other hand an issuing magistrate is entitled to presume that the officer making the application has a settled view as to the content of the warrant he or she is applying for, and the draft represents that view. That is not always going to be the case, and may be an explanation for one of the issues I encountered.

The paragraphs in the template which have spaces requiring completion are as follows:-

(1) The name of the applicant.

(2)The officer 'primarily responsible for executing the warrant'

(3)The alleged offence in respect of which the warrant is issued

(6)(a)'specified premises warrant', indicate surveillance device(s) to be authorised for use.

(6)(b) specify premises in which the warrant will authorise the use of the surveillance device(s)

(6)(c) specify any other premises which the warrant will authorise entry to.

(6)(d) any conditions subject to which the premises may be entered

(7)(a) 'specified objects warrant', indicate surveillance device(s) to be authorised for use.

(7)(b) list object(s) which warrant will authorise surveillance devices to be used on or in.

(8)(a) 'specified persons', conversations/activities and geographical location warrant. Indicate surveillance devices.

(8)(b)(i) name of person if known etc

(ii) or person whose identity is unknown

(9) cross jurisdictional, not applicable to matters under review.

(11)Conditions imposed on the use of the device

(12)Conditions under which the premises may be entered.

(13) the date of issue of the warrant

(14) the time of issue of the warrant

(15)The period of time in which the warrant is in force.

(16)The period of time in which the section 29 report is to be made.

All the paragraphs which require completion, details or information are required by sections 12 and 13 of the Act. Paragraphs 1-9 and 15 should be completed by the applicant as part of the documentation submitted to the Court.

The completed Application, affidavit and draft warrant are, after checking, submitted

electronically to the Magistrates Court when an appointment is obtained, usually by telephone call, for the matter to be heard by a magistrate. The experience of the officers involved in making the applications for the 19 warrants I examined was, with few exceptions, that the hearing appointment was made for the day following the making of the request and the lodgement of the documents.

HEARING APPLICATIONS FOR AND ISSUING WARRANTS

The 19 warrants issued during the period covered by the Terms of Reference were mostly, 16 in number, issued in Hobart, while 3 were issued in Launceston. This is understandable. The main prison facility, Risdon, is located in Hobart as is the Hobart Reception Prison, while in Launceston there is only the Reception Prison.

The practise for swearing affidavits accompanying the application varied. In Launceston the affidavit was sworn before a court officer before the hearing time. In Hobart most were sworn before the magistrate by whom the application was considered.

The hearing of the applications was not recorded, and, in accordance with the Act, there was no person, other than the magistrate involved with the applicant. One application, dealt with after-hours was, conducted at the home of the magistrate on a Sunday. Infrequently a magistrate required a condition to be included in the warrant, which necessitated a return appointment before the magistrate. There were few instances where clarification of information was sought and the time estimates given for the hearings ranged from 10 minutes for one matter up to 40 minutes.

The responses from the 16 officers I interviewed, (some officers were involved in applications for more than one warrant), indicated that they felt that the magistrates had read the papers and were in touch with the application and what was being sought.

The form of draft warrant presented to the magistrate will contain sections which require consideration by the magistrate, for adoption, completion or deletion.

I have indicated on page 23 those paragraphs which should be completed by the applicant prior to presentation. Arguably, for completeness, paragraph 4 (b) and (c) (unsworn and remote applications) should be deleted if they do not apply to the application process. I have indicated that none of the 19 warrants under consideration were so affected, yet not one of the warrants had those sub paragraphs deleted. I would prefer to see those paragraphs deleted.

The statements contained in paragraph 4(a) and 5 (a)-(e) are all prerequisites for the magistrate under section 12 as explained when I considered that section. They are mandatory.

The magistrate has a discretion as to whether to impose conditions concerning entry of specified premises (paragraph 6(d)), the use of the surveillance device (para. 11) and entry to premises generally (para. 12). These paragraphs are left blank for the magistrate to complete. In only one warrant was a condition or term inserted. The rest were left blank or noted “Nil”, “N/A” or marked with a diagonal line. All such notations appeared to be by the magistrate, some were initialled.

The remainder of the warrant, which should be completed by the magistrate before signing, is contained in paragraphs 13 and 14, the date of issue of the warrant and the time of issue.

The period of time that the warrant is in force for (para 15) and the time in which the section 29 report is to be made (para 16) are completed in the template to reflect the maximum time a warrant can be in force under the Act without extension, 90 days (s. 12(1)(b)(ix) and a time of 60 days for making the section 29 report.

I will comment further on my examination of the 19 warrants, but it is sufficient to mention at this stage that because the Act permits the issue of warrants with such wide scope, as observed by Justice Brett in the Thompson decision (see page 20), care should be taken in drafting the terms of the warrant presented to the magistrate for completion.

INSTALLATION OF SURVEILLANCE DEVICES AND RECOVERY OF RECORDINGS.

The process of surveillance device installation, operation and recovery of recordings varies, depending on the location and circumstances surrounding the activity under surveillance, and the investigators interviewed, who applied for the warrants I examined, reported that once a warrant authorising the use of a surveillance device is obtained a copy of the warrant is delivered to TSS, who instal the device(s) in the locations and, if recorded material is obtained from the targeted source by the use of the device TSS provide the investigator with a useable recording indicating that it was the only copy. The device is retrieved and any recording on the device(s) used in the surveillance is then wiped and the device then restored for availability as a cleaned device for the next task.

I will be examining this process when I consider the Thompson matter and the other files I have examined.

REPORTING TO THE SUPREME COURT OR MAGISTRATE UNDER SECTION 29

Under s 29 of the Act there are mandatory reporting requirements.

The officer to whom a warrant is issued or the person who is primarily responsible for executing a warrant must make a report, which complies with the requirements of that section, to the Supreme Court or the magistrate who issued the warrant. The report must be made within the time stated in the warrant, a requirement under s 12, or within the term of the warrant itself, if the warrant is revoked.

I attach, marked 'C' a template for the Section 29 report. I will comment further on this process later in my report when I consider safeguards in the system, but it is important to note some features of the report and the Compliance and Monitoring provisions in Part 5 of the Act

The s 29 report is, importantly, a report to the issuing officer and it provides sufficient information to the issuing officer to enable that officer to assess the outcome of the surveillance operation which was authorised by the issue of the warrant. The report must:-

"S 29(3)(a) state whether the warrant was executed; and

(b) If it was executed :-

(i) state the name of the person primarily responsible for the execution of the warrant; and

(ii) state the name of each person involved in the installation, maintenance or retrieval of the surveillance device; and

(iii) state the kind of surveillance device used; and

(iv) state the period during which the device was used; and

(v) state the name, if known, of any person whose conversation or activities were overheard, recorded, monitored, listened to or observed by the use of the device; and

(vi) state the name, if known of any person whose geographical location was determined by the use of a tracking device; and

(vii) give details of any premises on which the device was installed or any place at which the device was used; and

(viii) give details of any object in or on which the device was installed or any premises where the object was located when the device was installed; and

(ix) give details of the benefit to the investigation of the use of the device and of the general use made or to be made of any evidence or information obtained by the use of the device; and

(x) give details of the compliance with the conditions (if any) to which the warrant was subject;

The section also requires information concerning any extensions or variations of the warrant and the reasons for those extensions or variations and further requires the report to contain information concerning retrievals of a warrant. None of the warrants I examined involved retrieval orders and I will therefore not detail those requirements.

It should be noted that s 29(5) provides that on receipt of the report the Supreme Court or magistrate may order that any information obtained from or relating to the execution of the warrant or any record of that information be dealt with in the way specified in the order. This indicates that further orders may be made by the issuing Judge or magistrate. No specific direction is provided in the Act and no orders were made under this section for any of the warrants I examined.

Division 2 of part 5 of the Act, Compliance and Monitoring, defines 'protected information' (s 32) which includes all the documentary material I have examined, applications for warrants, affidavits in support, warrants issued and section 29 reports. S.33 of the Act prohibits communication or publication of protected information, with significant penalties for breaches, unless such publication or communication is permitted under s.33. For this reason an amendment of the Act was required to enable this Review and reporting to be undertaken. I will return to s.33 when I consider Safeguards.

There are record keeping obligations imposed upon the 'chief officer' of a law enforcement agency under Ss. 37, 38 and 39 of the Act, including the obligation to keep records of the destruction of records undertaken under s. 34. These provisions are important because they enable the 'inspection entity' (in Tasmania the Ombudsman) to at least once in every 12 months inspect records of a law enforcement agency to determine the extent of compliance with the Act by the agency and law enforcement officers of the agency (s. 41(1)) and report in writing to the Minister on the results of that inspection and to include a report on the comprehensiveness and adequacy of the records of the agency and the cooperation by the agency in facilitating the inspection of the those records (s. 42(1) and (2)).

The Minister is required by s.42(3) to lay a copy of that report before each House of Parliament within 15 sitting-days from the day on which the Minister receives the report. This compliance inspection and reporting is the last safeguard provided for under the procedures and requirements in the Act.

THE THOMPSON DECISIONS AND THE REVIEW.

STATE of TASMANIA v. THOMPSON [2022] TASSC 53 (28 March 2022)

TASMANIA v. THOMPSON (No 2) [2022] TASSC 55 (28 July 2022)

These decisions, referred to on page 1 of this report provide background for the decision to undertake this Review. I will examine both decisions to better explain and, hopefully, provide understanding of certain aspects of the Review.

The prosecution of Jeffrey Ian Thompson ("Thompson") for two counts of perverting justice is linked to the second appeal by Susan Blyth Neill-Fraser (Neill-Fraser") against her conviction of the murder of her partner Robert Adrian Chappell ("Chapell") on or about 26 January 2009 for which she obtained leave on 21 March 2019 under the 'fresh and compelling evidence' amendment of the appeal provisions of the Tasmanian Criminal Code.

The Terms of Reference/Scope document do not, nor should they, extend the scope of this Review to require consideration of any aspect of the trial of Neill-Fraser. The charges against Thompson, and a co accused, Stephen Gleeson ("Gleeson"), concerned allegations that they, and others, had endeavoured to create a false trail of "fresh evidence" to exculpate Neill-Fraser and implicate others in the murder of Chappel and that false trail was to become part of the fresh and compelling evidence at the Neill-Fraser appeal hearing.

In the early hours of the morning of 21 February 2017 a Tasmanian woman, Karen Keefe ("Keefe") had been arrested by police in Hobart. During the process of arresting and charging Keefe police became aware that she had recently travelled to Melbourne and provided a statement to assist Neill-Fraser in her second appeal against conviction. The circumstances of Keefe's journey to Melbourne, that she appeared to have received payment for what she had done and information Keefe volunteered caused police to suspect that Keefe was involved with others in a conspiracy to create a false evidentiary trail to assist Neill-Fraser. In 2016 Keefe had been serving a term of imprisonment in the Women's Prison Risdon where she befriended Neill-Fraser, a fellow inmate, and had expressed a desire to try to help her. She had been released from prison in December 2016, but after her February 2017 arrest was returned to prison where Neill-Fraser was still an inmate.

At about the same time, Gleeson, later to be charged along with Thompson, was serving a term of imprisonment in Risdon Prison, medium security section.

Legal representatives of Neill-Fraser were, during this time, preparing the fresh and compelling evidence case for Neill-Fraser's application for leave to appeal, the first legal step towards her appeal

under the amendments to the Criminal Code permitting a second appeal against conviction based on 'fresh and compelling evidence.' A hearing date had been set for 25 July. Visits to Hobart and Risdon Prison by lawyers and others, including a documentary film maker, were increasing in frequency.

The Tasmania Police operation to investigate the alleged conspiracy was established. The officers involved were located in a secure operations room at Hobart Police Headquarters where a coded key pad limited access to the room to those members of the investigative team, who alone knew the code. There were 7 detectives in the team which was given the operation name "Operation Ransack 2". Persons I interviewed who were not members of the Ransack 2 team told me that they had to 'knock' to gain entry to this room.

In late May 2017 the DPP, Mr. D G Coates SC, wrote to the Commissioner of Police and advised that he had been approached by a Melbourne based QC and Thompson, a local person with a legal qualification, who had provided further material which would be pertinent to the hearing on 25 July. This material included statements from Meaghan Vass, a witness in the trial of Neill-Fraser in 2010, and Gleeson, alleging that other persons were on the yacht "Four Winds", the scene of the murder of Chappell, and two men named in that material committed the murder.

Documents supplied to me as part of my Review show that when the communication from the DPP was received it was determined by Police that this new information should be investigated but separately from the Ransack 2 team which was focussed on a suspected conspiracy. The new material was to be investigated and assessed for its reliability as fresh and compelling evidence. The investigation was given the code name "Operation Ransack 2A" and was established in an office separated from the Ransack 2 secure room and staffed with investigators from outside Hobart CIB who had not been involved in Ransack 2. While this team was operating separately from Ransack 2 the sharing of information was anticipated.

Investigators in the Ransack 2 operation had been obtaining warrants for the installation of surveillance devices and utilising other investigative tools, including telephone intercepts, to assist in determining the extent of the conspiracy and the identity of those involved. The covert element of this investigation was extensive.

The warrant which Justice Brett examined in the Thompson trial and was the subject of his rulings was in fact the fourth surveillance device warrant obtained by the Ransack 2 team, the other three were all obtained earlier and concerned meetings or appointments which were to take place in the Women's Prison. The first warrant was issued on 9 May to record a meeting on 11 May. That meeting did not take place. The fourth warrant, anticipating a meeting between Tompson and Gleeson, was issued on 13 June for meetings anticipated to take place on 16 June in a meeting room located in the Medium Security Prison.

The meetings, communications and appointments investigated by Ransack 2 detectives, intelligence gathered by both teams and earlier statements obtained in the murder investigation resulted in the Ransack 2A team concluding that the origins of the fresh evidence they were investigating were linked to the conspiracy which the Ransack 2 team was investigating. The evidence from the sources provided by the DPP was therefore not fresh and compelling.

The first Thompson decision, referred to above, concerned a challenge to the lawfulness of the surveillance device warrant issued on 13 June, one ground being that the warrant was not valid on its face. This submission was upheld by Justice Brett.

VALIDITY OF THE WARRANT.

The warrant issued by the magistrate on 13 June 2017, in paragraph 3, stated that "The alleged offence in respect of which the warrant is issued is Conspiracy, contrary to Section 297(2)".

His Honour, in finding that the warrant was invalid on its face concluded :-

Par 23 "The trouble in this case is, I think, the one I discussed with counsel during argument and that is that on its face, the warrant purports to confine conspiracy by reference to a provision. If it had said "By reference to s. 297", I think it highly arguable that it would not be objectionable. It would simply be saying that it authorises surveillance of conversations that refer to any agreement that can fall within the ambit of that section. The problem here is that there has been an apparent attempt to narrow down the ambit of the crime under investigation, but it is completely impossible for a reader of the warrant to identify the relevant subparagraph of s.297(1) defining the offence having regard to s,297(2).

24. "Section 297(2) does not refer to a crime. It says, "Married persons are not criminally responsible for any conspiracy between themselves only." The section has no relevance to the specification of an offence. A person reading it might say "Well the magistrate, the issuing officer, was obviously referring to something in s.297." However, s.297 can refer to various specific forms of conspiracy and it is clear that the issuing officer had in mind to refer to something, possibly one of those specific forms of conspiracy. It is impossible for me, or for anybody reading the warrant, to determine which offence is being referred to, and I am satisfied that that does lead to invalidity."

His Honour's finding that the warrant was invalid on its face brought in to play s 138 of the Evidence Act 2001 which provides that evidence which is obtained in contravention of an Australian law (and using a warrant which was invalid on its face to obtain that evidence creates such a situation) , is not to be admitted unless the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained. The exercise of His Honour's discretion under s 138 is the subject of the second decision referred to above (see Tasmania v. Thompson (NO 2) [2022]TASSC 55 (28 July 2022).

In deciding whether or not to admit the evidence of the recording of the meeting between Thompson and Gleeson in the professional meeting room at Risdon Prison on 16 June 2017, His Honour was required to take in to account a number of matters contained in s 138(3) of the Evidence Act including,"(a)the probative value of the evidence", "(b)the importance of the evidence in the proceeding" and, amongst others, importantly "(h) the difficulty, if any, of obtaining the evidence without impropriety or contravention of an Australian law." The prosecution carried the onus of satisfying His Honour that he should exercise his discretion in favour of admitting the evidence.

Senior counsel for Thompson, David Edwardson QC, submitted that the material provided by the police (in support of the application for the surveillance device warrant) did not objectively justify the issue of the warrant, and this was a fundamental consideration in exercising the discretion under s 138. The prosecution submitted that this was not a relevant consideration and that His Honour should have regard to the conduct of the police when assessing the gravity of the contravention.

Justice Brett agreed with defence counsel

"10. I agree that the question of whether the affidavit material was objectively sufficient to support the magistrate's decision to issue the warrant may be a relevant consideration. It probably does not properly fall under the question of the gravity of the impropriety, but is relevant to the closely related issue specified by subpar (h), the difficulty of obtaining the evidence without contravention. If on the material presented to the magistrate, a warrant could not reasonably have been issued, and hence the conversation could not have been lawfully recorded, then this would be a strong factor supporting exclusion. I agree with the defence that this is so, irrespective of the apparent attitude taken by the magistrate. Having regard to the actual unlawfulness of the recording, it is a matter for me to determine whether the conversation could have been lawfully recorded had a valid warrant been issued. On the other hand, a conclusion that the magistrate's decision to issue the warrant was a reasonable one having regard to the evidence presented to him, would be a factor supporting the admission of the evidence. Accordingly, it is appropriate to consider the sufficiency of the material.

"11. Defence counsel submitted that, in this context, the failure of the prosecution to call the magistrate to give evidence on the voir dire was an important, if not fatal, flaw in the prosecution's case. I disagree with this. The question of whether the warrant could have been issued lawfully can adequately be determined on the basis of the material that was provided to the learned magistrate. It is obvious that the magistrate was persuaded to issue the warrant and it is adequate for me to consider whether this decision was a reasonable one on the basis of the relevant material. It seems to me that any further consideration of this question cannot inform the exercise of my discretion in any meaningful way."

I have included his Honours reasoning in paragraphs 10 and 11 in full for two reasons:-

(a) I have not sought to interview any of the magistrates who issued the 19 warrants I have examined and I believe that Justice Brett's reasoning supports that decision. I do not believe that the authority given to me to conduct this Review permits me to do so in any event, but there is sufficient material contained in the files I have examined to enable me to determine whether the information provided to the magistrates provides sufficient detail to respond to paragraphs 2 and 3 of the Review Terms of Reference, and
(b) His Honour's reasoning supports the decision I have made to not limit my Review to the question of risks of capturing private conversations and measures to mitigate those risks but rather, for completeness, to examine other information provided to the magistrates in the sense that if this information did not satisfy statutory requirements then a warrant should not have issued, even if valid on its face. A step unlikely to be available in the legal process followed by Justice Brett, but certainly helpful in answering questions raised about adequacy in the Terms of Reference.

The examination of the Thompson decision will also enable me to address concerns raised with me about evidence given to and comments made by His Honour.

The affidavit in support of the application for the surveillance device warrant issued on 13 June, when compared with the affidavits filed in support of the first three warrants obtained by the Ransack 2 detectives, contains details of the evidence compiled as the investigation progressed and complements the evidence referred to in the affidavits filed in support of the first, second and third warrants. It is 51 pages long and while containing evidence provided in support of the earlier warrants adds evidence gathered subsequently.

In Justice Brett's second decision (above) he considered the evidence relied on by the deponent of that affidavit to support the requirement of s 9(1)(a) and (c) of the Act, the law enforcement officer's 'reasonable grounds for a suspicion or belief that some persons named in the affidavit had entered in to a conspiracy to pervert the course of justice' and that the use of a surveillance device is or will be necessary in the course of the investigation for the purpose of enabling evidence or information to be obtained of the commission of the relevant offence.

In paragraph 15 Justice Brett concludes :-"Notwithstanding these difficulties the affidavit does, in my view, set out evidence sufficient to satisfy a magistrate that there are reasonable grounds for a suspicion or belief that at least some of the persons referred to in the affidavit have entered in to a conspiracy to pervert the course of justice, In particular, the evidence asserted in the affidavit provides a reasonable basis to conclude that:

(a)Karen Keefe and Ronald Mackenzie formed an agreement to pressure or influence Megan

Vass to provide a version of events of the night of Australia Day 2009, when Mr. Chappell went missing inconsistent with the evidence she provided for the original trial.

(b) As a result of their actions, Vass signed a statutory declaration on 27 April 2017 in which she asserted that she was on the yacht on the relevant night with other unnamed persons and that ms. Neill-Fraser was not present.

(c) Keefe and McKenzie were expecting a substantial payment in exchange for persuading Vass to make the relevant declaration.

(d) Colin McLaren was aware of the efforts of Keefe and McKenzie to persuade Vass to change her evidence. There was also evidence which connected McLaren to a payment of $3,000 to Keefe.

(e) Gleeson had made statements that police believed were false. In particular, on 13 September 2016, he signed an affidavit stating that he thought Paul Rowe was involved in the disappearance of Mr. Chappell. On 8 May 2017, he made a more detailed statutory declaration in which he repeated this assertion and stated that a young girl and male by the name of Adam Yaxley were present at Marieville Esplanade, and discussing breaking in to yachts, on the relevant night. Police believed that these statements were false, because they were inconsistent with information provided spontaneously by Mr. Gleeson to investigating police on the night of Mr. Chappell's disappearance, and further, came about in the context of 17 separate visits to Mr. Gleeson in prison by McLaren, Eve Ash and the accused (Thompson) since July 2016. The evidence also established a possible link between Keefe and McKenzie on the one hand, and Gleeson on the other because of comments made during recorded telephone conversations and, further, the connection provided through McLaren, Ash and the accused."

His Honour then examined the evidence in the affidavit which supported the deponent's belief that the meeting for which the surveillance device was sought would provide evidence or information in respect of the relevant offence. His Honour concluded that it did.

Although, in the end, his Honour determined that he would not, in the exercise of his discretion, admit the evidence of the conversation between Gleeson and Thompson, his consideration of those evidentiary requirements of a supporting affidavit is relevant to my consideration of the 'information' aspects of the process, which I will return to.

The meeting between Thompson and Gleeson and their conversations did not include the witness from the trial, Vass. Other evidence gathered by the investigators provided a sufficient basis to challenge the fresh evidence account being put forward through Vass, and Gleeson at the pending appeal.

At the hearing of the second appeal Vass gave evidence to establish the first particular of fresh evidence in support of the appeal :-

“That there is fresh and compelling evidence that;

1.1 Meaghan Vass has boarded the Four Winds, and the deceased was attacked while she was on board.”

Under cross examination Vass recanted that evidence and stated that her account was not correct and before cross examination had concluded Senior Counsel for Neill-Fraser withdrew that particular of fresh evidence from the appeal and no longer relied upon it, limiting the fresh and compelling evidence element of the second appeal to evidence of an expert concerning DNA evidence. That appeal has been heard and dismissed.

PRIVACY AND THE EXECUTION OF THE WARRANT

Under this heading His Honour considered the affidavit evidence provided to the issuing magistrate and the evidence on the voir dire from two police officers.

Examining His Honour’s reasons for declining to admit the evidence obtained from the surveillance device will not only inform the aspect of privacy in my Review but also enable me to consider matters of concern raised by His Honour and counsel who have spoken to me.

Section 11(2) of the Act requires that an issuing magistrate, “in determining whether a surveillance device warrant should be issued” must” have regard to the extent to which the privacy of any person is likely to be affected”.

The affidavit filed in support of the application, which sought authorisation for the use of a listening device and optical surveillance device on or in premises, namely the visitor meeting rooms utilised by Stephen John Gleeson 23.12.59 at the Risdon complex”, addressed this issue, in the numbered paragraphs, as follows:

“[18] The matters relevant to how much the privacy of any person is likely to be affected by the issue of a surveillance device warrant are set out below. Having regard to those matters the privacy of persons other than Gleeson would not be unduly interfered with.

[19] Any incidental interference with the privacy of any person would be justified given the seriousness of the matters under investigation:

(a) Police can obtain information relating to times and dates of relevant meetings and can isolate the monitoring of any listening device product to meetings relevant to this investigation. Therefore any personal or legal visits between inmates and visitors not directly involved in the investigation will not be monitored.

(b) Police do not intend to monitor visits that obviously only relate to professional legal visits."

At the hearing of the voir dire two police officers gave evidence. The detective from Operation Ransack 2 who applied to the magistrate for the warrant which was issued, and swore the affidavit in support and an officer from TSS who installed the two devices in the meeting room as authorised by the warrant.

His Honour concluded that "it is apparent from the evidence of the police officers that they were not able to be any more precise as to the meeting room, and were reliant on prison authorities to identify the relevant room. However, both officers were aware, and the magistrate must have been aware, that the professional meeting rooms in question would in the usual course be utilised by lawyers and clients to conduct conversations protected by legal professional privilege. There was a high probability of many such meetings over the proposed life of the warrant, 90 days. Indeed this is the factual assumption that underlies par [19]. There was no other information provided in the affidavit concerning the anticipated use of the room."

The TSS officer who installed the surveillance devices in the meeting room gave evidence that he attended the Prison on 13 June and installed two devices, an audio-visual device and an audio only device. The audio-visual device was capable of being operated, turned off and on remotely and was capable of transmitting sound and image to a laptop computer he had installed in the Ransack 2 room referred to earlier to enable the meeting between Thompson and Gleeson to be observed and heard. The audio only device recorded to a hard drive, was not capable of being operated remotely and could not transmit. The only way of turning this device on or off was by physically attending to the device in the room.

The TSS officer informed the Court that when he installed the devices he activated them so that they would record continuously, explaining that his reason for setting both devices to continually record was that "technology, as it can be, can be temperamental at times, and in the event of failure it's impossible to actually contact or make changes or turn on and off devices at will, so to eliminate those issues, it was operated like that, and also as well, to actually access the prison at short notice to do something expediently is inherently difficult to achieve and hard to do."

Three days after the meeting between Thompson and Gleeson took place at the Prison, was viewed in the Ransack 2 Operations Room and recorded on the devices, the audio/visual device malfunctioned and had to be restarted. The functioning was checked by the TSS officer in the meeting room on 21 June when he also downloaded that portion of the recorded content of the two devices which had recorded the meeting, recording them separately to two discs which he then passed to the officer who had applied for the warrant.

The two devices continued to record until they were retrieved on 17 August, two months after the meeting between Thompson and Gleeson. The devices were taken back to the TSS offices and

“wiped,” or deleted, any recorded content to have them ready for installation in other investigations. Both officers gave evidence that they did not attempt to access any of this recorded material before the devices were wiped.

Both Senior Defence Counsel David Edwardson QC, in submissions, and His Honour in comments and his reasons for declining to admit the evidence, expressed concern at this evidence and I will set out in full that portion of His Honours Reasons for ruling the evidence inadmissible.

“ A (The TSS officer) gave evidence that the practice was that the product remained recorded on the devices until they had been retrieved. At that time, all recordings on the devices were deleted so they could be used for other cases. That is what occurred in this case.

“During the course of his evidence, I asked A whether he had the capacity to switch the devices on and off so as to prevent them recording except at times relevant to the investigation. He accepted that they had this capacity. The surveillance device with both audio and visual recording capacity could be switched on and off remotely, but direct access to the device itself was required to achieve this on the other device. When I asked why this did not occur, he indicated that they were left running in case “technical issues arose or there was insufficient time to get in to the prison to access the equipment prior to the scheduled meeting. He indicated that there was a degree of complexity involved in arranging access. He was dealing only with certain correctional services officers and delays could arise because those officers were off shift or absent for other reasons. I must say that I did not find this explanation persuasive. I have no doubt that in many cases, particularly where listening devices are installed in premises over which police or other related authorities have no ongoing control, such as private residential premises, there is no practical option but to leave the devices running continually. It would be impractical, if not impossible, to gain covert access to the devices regularly and in any event, it would be highly unlikely that the monitoring authorities would have sufficient notice of relevant conversations. However, that was not the situation in this case. As B (the officer who applied for the warrant) explained in par[19],(of his affidavit), and as is obvious in any event, police were always going to have significant notice of any relevant conversation and be able to gain risk free covert access to the relevant room with the cooperation of the authorities. It is obvious that any meeting between Gleeson and any person of interest would need to be scheduled with the prison authorities well in advance. The location of the meeting would be completely under the control of those authorities. I accept that for security reasons, police would only have been dealing with a limited number of prison officers, and would have been concerned to keep this contact to a minimum, but I cannot accept that in the highly controlled environment of a prison, there would have been any real difficulty in police obtaining notice of meetings and access to the equipment in a timely way. It seems to me that this was precisely the point that B was making in par [19] of the affidavit. Further, Constable A was, in any event, required to access the devices in situ on one occasion because of a malfunction. Indeed, one would think that attending the devices prior

to any relevant conversation would guard against, rather than increase the risk of unforeseen failures in the equipment. I think it is far more probable that pressure of work meant that it was easier to leave the devices running than to switch them on and off before and after each relevant conversation. A hinted that he was under a considerable amount of time pressure because of other work commitments.

“The upshot of all this is that these devices were left to continually record throughout the entire period between 15 June and 17 August 2017. I have no difficulty inferring that during this time there would have been many sensitive and privileged conversations between lawyers and their clients, and perhaps other private conversations which were completely irrelevant to this investigation and not authorised for recording by the warrant. The persons concerned would have had absolutely no idea that their conversations were being recorded and were capable of being monitored, in real time, by police and other authorities. B said that he did not monitor any other conversation nor did he request the download of any product. A said that he did not arrange monitoring of any other conversation nor download any other product. I accept the truth of this evidence. However there were at least five members of the investigation team and a number of members of the technical service unit (TSS), all of whom had access to the relevant equipment. The only security applied to access to that material seems to have been that the monitoring equipment was within the investigation room which required passcode access. The passcode, according to B, was known to all members of the investigation team. A technical services officer had to request access to the room, but this could have been given to them or any other person by any member of the investigation team. No one else from either unit was called to give evidence nor was any evidence presented to exclude the possibility that any other material had been accessed by authorities. I am not suggesting for a moment that this did occur, but clearly there was that potential.

“The real problem here is that this information was something that the magistrate was required to take into account when deciding whether to issue the warrant, and if so, on what terms and conditions. These considerations had real potential to interfere with the privacy of other persons and this is a mandatory consideration for a magistrate when determining whether to issue the warrant. Had the magistrate been made aware of these matters he may well have declined to issue the warrant or at the very least placed conditions upon it. For example, a simple condition which required the authorities to switch the recording devices on only for the duration of any arranged and notified relevant conversation would have taken care of this problem. The fact that the magistrate was not told about this, and that police in any event did not implement these measures, is a matter of significant concern.

“I accept that in par[19], B did not deliberately mislead the magistrate. He states that police will not “monitor” any “listening device product.” These terms can be understood in light of A’s explanation. But this, of course, was not provided to the magistrate. Perhaps it was assumed that this was self-

explanatory, but such an assumption was unjustified. Given the real risks to privacy arising from the near certainty that unrelated private and privileged conversations would be recorded and capable of being monitored during the life of the warrant, far greater detail should have been provided to and considered by the magistrate before issuing the warrant.

“Having regard to all of this evidence, I am satisfied that the warrant issued by the magistrate did not satisfactorily respond to the risk to privacy inherent in this proposal. The warrant permitted use of a surveillance device in “visitor meeting rooms utilised by Stephen John Gleeson….. at Risdon Prison Complex.” Although the magistrate could have imposed further conditions on the use of the warrant to ensure that police complied strictly with the intention asserted by B in par [19] of the affidavit it contained no conditions whatsoever. It may well be that the magistrate relied on B’s assurance in par[19] and thought that the ambit of the authorisation adequately responded to privacy concerns by restricting the use of the devices to premises described as ‘visitor meeting rooms utilised by Stephen John Gleeson”. If the magistrate did think this, then his approach was flawed.”

His Honour then explained the ambiguity of the ‘rooms’ description and declined to accept a submission from the prosecution that the police were acting in compliance with a warrant which they believed was valid and there was no evidence that any other conversations were recorded or downloaded by any other police officers.

His Honour continued:-“ The difficulty I have with this submission is that I am simply not persuaded that police took sufficient care to either inform the magistrate of the proper operation of the system not to obviate any risks related to the potential for the recording and/or the monitoring of unrelated private or privileged conversations. The public interest in ensuring that such conversations are protected from unlawful surveillance by law enforcement authorities is of significant importance. Accordingly, while it appears that police did not deliberately set out to break the law, there was also an obvious misunderstanding or ignorance of the significant risks inherent in their task and a casual and incomplete approach to the identification and minimisation of any such risks. The protection of the privacy of others using the room could have been easily achieved by activating the devices so that they recorded only the relevant conversations. Because of the importance of this question of privacy in the circumstances of this case, I regard this as a significant factor telling against the admission of this evidence.

His Honour then concluded :-

“Balancing all the above factors, I am not satisfied that the desirability of admitting the impugned evidence outweighs the undesirability of admitting evidence obtained in the manner described. In making this determination, I have taken in to account all relevant factors including the seriousness of the alleged crimes, and the effect of the exclusion on the prosecution case. However, ultimately, I am heavily influenced by the considerable risks to privacy which were inherent in this proposal for covert

surveillance, and the failure of police to consider and properly address those risks and to fully inform the magistrate of the circumstances of the surveillance which compounded those risks. In my view, had the magistrate been properly informed then even if a valid warrant had been issued, it is highly likely that it would, or at least it should have contained conditions sufficient to properly obviate the said risks. The evidence which was presented fell far short of satisfying me that police had any significant insight in to these problems and their importance, nor that anything has been done since to address similar situations. I accept that there will be a limited number of cases where concerns of this nature will arise, that is the potential for recording of privileged as well as private conversations unrelated to the investigation, and where there are simple practical means available to restrict surveillance to relevant activity. However, the importance of ensuring the protection of privacy in respect of unrelated and privileged conversations during the course of covert surveillance, satisfies me that the balance in this case falls in favour of exclusion."

I have included this extensive portion of His Honours reasons because it contains not only the elements of the decision, but also much of what is fundamental to the consideration of an application for a surveillance device warrant for the installation of a device in a prison or other person sensitive location. This will inform the considerations in the balance of this Report. The passages also detail concerns expressed by His Honour, some of which have also been raised with me by a number of people, some of whom I have interviewed.

I will outline the process I followed for this part of the Review and confine the remainder of the section to identifying those concerns and examining them. I will, after concluding this section, return to consider all 19 warrants and the specific aspects of the application process relevant to the Review.

THE REVIEW PROCESS UNDERTAKEN IN CONSIDERING THE DECISIONS IN THE THOMPSON CASE.

(a) I interviewed all 5 officers serving in TSS across the relevant period. The operation of the surveillance devices and the functioning of the transmission to the remote facility in the Ransack 2 operations room were within their sole control and operational oversight throughout the period of continuous recording, and they were responsible for the retrieval of the devices from the meeting room.
(b) On occasions, while progressing the Review, I interviewed a senior TSS officer and examined records and files relevant to all 19 matters, particularly the 4 warrants issued during the investigation of the alleged conspiracy to pervert the course of justice in May/June 2017. It was important to understand the operational exchanges and responsibilities of investigators and TSS officers not only during the Ransack 2 investigation but also throughout the period covered by the Review.

(c) I visited Risdon Prison and inspected the professional meeting room in which the Thompson and Gleeson meeting occurred, and examined other meeting/contact visit facilities at Risdon Prison. That room is no longer used as a professional meeting room but I was able to assess the location of the room and the visibility of the path which would have to be taken to access that room. I was accompanied by a former TSS officer who had also assisted in accessing the room at the time of the Ransack 2 investigation.

(d) I inspected the room used for the Operation Ransack 2 secure facility. The room was not being used at the time but I was able to assess the visibility of the laptop and screen from any position within the room. The screen is a fixed accessory.

(e) I interviewed 7 of the 8 officers who served on the Operation Ransack 2 investigation and worked in that room. (One officer was unwell and not able to be interviewed). I assessed the breadth of the evidence I had from the 7 interviews and was satisfied that I had covered a sufficiently wide base of activity in that room during the operation.

(f) I read the transcripts of the evidence of Officers A and B on the voir dire and the submissions of counsel.

(g) Before interviewing the 12 officers in TSS and CIB I spoke with both senior counsel involved in the voir dire, David Edwardson KC and Linda Mason SC, two local defence counsel Fabiano Cangelosi, of counsel and Cameron Scott, of counsel who I was aware had concerns and also the Hon Meg Webb MLC, and Greg Barns SC. All these people readily made themselves available to discuss their concerns and understand the breadth of my review. Two had specific concerns, they believed they had used the room which was under surveillance during the time the devices were recording, others were concerned about the shortcomings which the Thompson decisions had disclosed and that the terms of reference of the Review were not broad enough. The fact that my Review would be confined to matters concerning warrants for use in prison when there were warrants issued for installation of devices in other locations which should also be considered.
I also spoke with most of these people a second time, after I had interviewed all police officers.

(h) I also undertook a review of one of the safeguard mechanisms within the Act, the Inspection Entity, which I will outline later in this Report as the outcome of that review is more relevant to the scope of the Terms of Reference which I will consider after examining the 19 warrants issued during the period covered by the Review.

THE EVIDENCE AND MATTERS OF CONCERN.

I will address those matters of concern to me, and raised with me by people I met with, as detailed on the previous page which are confined to the evidence and outcomes in the Thompson case. The scope of the Review is wider than this case and will permit me to adopt a course which was taken in Thompson, which I will follow, but firstly I will address the concerns arising from this case.

While, ultimately, the reason for refusing to admit the recorded evidence of the Thompson/Gleeson meeting was the continuous running of the recording devices in the meeting room after that meeting when the magistrate, in considering the warrant application, had not been informed that this would happen. The invalidity, on the face of the warrant, provided the Court with the opportunity to go behind the warrant and, in the exercise of it's discretion under s. 138 of the Evidence Act, consider the evidence and those matters I have referred to. I will follow a similar course with all 19 warrants issued even where the warrant is valid on its face. I am satisfied that the Terms of Reference permit that.

The fact that recording devices were running constantly in a professional meeting room at the Prison is of concern generally and it is a matter which concerns me. However, more specifically, it concerned lawyers and others who had used the room for meetings and consultations which were not related to the alleged conspiracy for which the warrant permitted the installation of the surveillance devices. For them the concern was one which required answers and reassurance about what was recorded and what has happened to the recordings.

The extent of the Review should therefore not only cover those matters contemplated by the Terms of Reference, but also address the concerns raised by the evidence and the Judge in the Thompson matter, and in turn raised with me. The concerns are wider than just one matter, as are my Terms of Reference and I will consider those matters after I have reported on my examination of all 19 warrants.

The narrower fields of concern from the Thompson case involve serious matters and answers must be provided, if they have not already. There is a significant public interest not only from my own concerns but manifested in the concerns expressed to me. In determining the extent of the problem, I must also consider public and judicial confidence in the processes followed in this area of authorised covert surveillance and, more narrowly, in reassurance to those concerned that privileged conversations were not downloaded or monitored.

The questions or concerns are:-

(i) Why Were Two Recording Devices Used?

The use of two different surveillance devices was sought in the application for the warrant. TSS officers had experienced technical problems with the audio/visual device's remote operation, as explained to the Court, where on occasion the remote turn off function resulted in the device not responding when attempts were made to turn it back on. So, as back up, the constantly running sound recorder was also installed. The audio/visual device also provided, if functioning, the capacity to remotely monitor the conversations between Thompson and Gleeson. The investigation of the alleged conspiracy was being conducted on a number of fronts, answers were needed quickly to determine the identity of any persons knowingly involved, other prison visits were occurring, telephone interceptions were being undertaken. Investigators needed to expeditiously determine the breadth of the suspected conspiracy.

When I examine the other warrants it will become apparent that the frequency of visits to the prison by covert operatives at this time was causing concern for the risk of disclosure, the full extent of which was not apparent to Justice Brett from the evidence he heard on the voir dire.

(ii) Why Were the Devices Set to Run Constantly (from mid-June to 17 August)?

My interviews confirmed the veracity of the explanation given to the Court that the technical issues with remotely stopping and attempting to re-start the audio-visual device and returning to the meeting room to turn the devices off and on was problematic because of availability of the officers at the Prison aware of the matter and concern that the secrecy of the identity of TSS officers was at risk of compromise with frequent visits to the prison.

> (On my visit to the Prison I observed that the room in which the devices were installed in 2017 is now an office occupied by two staff members and the other, smaller, meeting room beside it is also used for other purposes. When I visited this part of the Prison I tried to assess the level of visibility an undercover TSS officer would face when attending that part of the prison. I noted 7 different prison staff who readily observed my visit. I also inspected other visitor facilities and noted slightly fewer staff in positions to observe that visit.) Further detail of this aspect of the Review will be provided when I consider the other warrants.

(iii) What is the likelihood that anyone monitored or recorded other meetings and professional visits to the room after the Thompson/Gleeson meeting and while the devices were still operating?

I am satisfied, that although still recording, no monitoring or downloading occurred. Shortly after the meeting took place on 16 June the monitoring lap top in the Operation room was closed and none of the 7 team members I interviewed saw or heard any transmission or play back through the system which showed any live or recorded monitoring. I interviewed all the 5 TSS members at that time and those in contact with the operation are confident that there was no further monitoring or downloading and when the devices were retrieved they were 'wiped' when returned to the office. The officer to whom the warrant was issued gave evidence on the voir dire and was not cross examined by experienced Senior Counsel for Thompson, David Edwardson KC, after Senior Counsel for the prosecution, received the following answers from that officer :-

"At the conclusion of the meeting what was done as far as the capacity to watch the live streaming of..of any further meetings?

"I don't believe we had the capacity post that meeting.

"So, explain that answer, why didn't you believe that?

"Well I never requested it again from the Technical Surveillance area and I was unaware of any other meetings to Mr. Gleeson, so I didn't make any request for the capture of those and until this week I was unaware that that device continued or functioned in any form.

"Okay. I will take you to that in a moment. But as far as the setup was concerned to enable you to watch anything that was occurring in the room, once that meeting concluded what actually happened to the capacity or otherwise to turn that on or off?

'Well it was all turned off and finished.

"So if you had wanted to watch another meeting again, what would you have had to do?

"I would have had to request technical surveillance services set-set it up again.

"Okay. You've just given evidence that you didn't, in fact, request technical surveillance unit to set it up again?

"Correct.

"Yeah. And you've also given evidence that until this week, I think, until recently, you were unaware of it continuing. Can you just explain, firstly, what was your understanding- your own understanding or belief, as to how further meetings between Mr. Gleeson and others, if in fact they were to occur, would be recorded?

"That that would require me to make application or request of technical surveillance again, to capture that meeting.

"Okay. And you've indicated – well what was your belief then as to the recording device and it's operational status?

"Well, I didn't believe it to be operating outside of our request.

"Okay. Were you aware, in your capacity as part of the investigating team of any other meetings that took place in that room, close to the 16th June?

"No, I was not aware."

This was the evidence of the person to whom the warrant issued, he was the officer primarily responsible for executing the warrant and a member of the team occupying the room in which the monitoring device was located. Taking in to account the answers I received to the questions I asked of another 6 members of the team working in that Operations room it is reasonable to conclude that the only transmission to that monitor was the one made on 16th June and there were no other viewings on that screen.

I am not seeking to question what was said by His Honour in his reasons, when referring to the fact that only two officers had given evidence as to the absence of any further recording and the limited access to the room where the monitor was…. that "no one else from either unit was called to give evidence nor was any evidence presented to exclude the possibility that any other material had been accessed by authorities. I am not suggesting for a moment that this did occur, but clearly there was that potential." His Honour did not suggest that it did occur.

It was that 'potential' which should have been explained for consideration by the magistrate who issued the warrant. Prosecuting Counsel at the trial made the decision to not call any other witnesses and, in light of the fact that Officer B's evidence, above, was not questioned or challenged in cross examination, I agree with that decision also.

I have devoted some time to considering this question because people are genuinely concerned that unauthorised monitoring and/or downloading of confidential conversations occurred. I am satisfied that while the devices continued to record no monitoring or downloading occurred and the recordings were deleted or 'wiped' without inspection.

(iv) Why was the Magistrate not informed of the Continuous Recording?

The person who swore the affidavit in support of the application for the warrant was an investigator and the exchange of information between him and the TSS officer did not detail methodology or technical information and he was clearly not aware that the devices would, in due course, be left to continuously record, once the meeting between Thompson and

Gleeson had been recorded. See his evidence above in (iii) and the form of the warrant, when issued and shown to the TSS officer, did not contain any limiting conditions, such as those envisaged by Justice Brett, which would have prevented or limited the prospects of such an outcome. The paras., [18] and [19], of the affidavit in support, referred to on page 34, reflect that state of mind. I will examine this issue later in this Report as it is relevant to other warrants I examined.

(v) What has happened to the recordings which were made on the two surveillance devices which operated until 17 August 2017?

They were wiped when retrieved and taken back to the TSS offices in Hobart. I have not enquired of the Prison authorities as to any schedule of meetings and appointments for the use of that room between 16 June and 17 August, I don't have authority to do so and I am satisfied that no recording was retained or examined by any police officer before deletion.

(vi) Is this likely to happen again?

No. Firstly the technology of recording devices now used is more sophisticated and reliable, avoiding the precautions of having the back-up of a continuously operating recorder which requires physical attendance to operate. Secondly, the internal review of warrant application procedures which was undertaken before I commenced this Review has introduced changes which, as I will explain later, will assist in preventing such an outcome in future. Thirdly, I anticipate that a recommendation I am making concerning continuing communication between investigators and TSS officers will further assist.

ACKNOWLEDGEMENTS.

I mentioned on page 40 the people with whom I had discussed matters of concern and issues arising within the scope of this Review. After interviewing in excess of 30 police officers I returned to speak with all but one of those people again. I wish to acknowledge and thank everyone I have mentioned for their assistance and their willingness to give of their valuable time, particularly cooperating with my schedule as the Review process evolved. They are all busy professionals and their input and assistance was extremely helpful.

THE TERMS OF REFERENCE AND THE WARRANTS UNDER REVIEW.

Under paragraphs 2, 3 and 4 of the Terms of Reference I am to consider:

2. The adequacy of information provided to issuing officers (magistrates) in applications for the surveillance device warrants within the scope of the Review in relation to:

i. the risk of the use of the device resulting in the capture of private conversations unrelated to the investigation

ii. proposed measures to mitigate the risk of capturing such private conversations and to prevent access to or retention of any such conversations.

3. The adequacy of any conditions or limitations imposed by issuing officers on warrants to mitigate the risk of capturing such private conversations and to prevent access to or retention of any such conversations

4. Compliance by Tasmania Police with any conditions or limitations referred to in 3 and the adequacy of any measures taken by Tasmania Police of its own volition to mitigate the risk of capturing such private conversations and to prevent access to or retention of any such conversations.

I have outlined in detail the provisions of the Act relevant to what I have been asked to review, and examined the reasons for the surveillance device product obtained in the Thompson case being ruled inadmissible. I have viewed all the documents in the 19 matters considered by the magistrates when hearing the applications for all the relevant surveillance device warrants and interviewed the authors of those documents.

As previously reported, there are 19 surveillance device warrants within the period covered by my Review, which now spans 12 years, from 1 January 2012. The crimes under investigation range from murder to drug trafficking and conspiracy to pervert justice to robbery with violence.

The years in which the 19 warrants were issued for installation of surveillance devices in a prison are as follows :-

2013/2014. 3 warrants

2016/2017. 6 warrants

2017/2018. 2 warrants

2018/2019. 7 warrants

2019/2020. 1 warrant

Total 19 warrants

All 19 warrants were issued by magistrates and 16 of the warrants authorised use of surveillance devices in Hobart either at the Hobart Reception (Remand) Centre or at the Risdon Prison. The remaining three authorised use of devices in the Launceston Reception Centre.

Two warrants were issued in 2013/14 for the one murder investigation in Hobart, the first warrant for a meeting which did not take place, that crime involved more than one suspect. In another matter, involving three suspects in two different prison locations and other suspects residing outside prison and in two states but meeting inside the prison, four warrants were issued in 2016/17, the first for a meeting which did not take place. In another matter involving two suspects in the one criminal enterprise three warrants were issued in 2018/19.

THE PROCESS OF APPLICATION FOR WARRANTS.

I have previously explained in summary the application process, which appears consistent in the two prison areas, Hobart and Launceston. An appointment is made through the court registry and the papers, application, affidavit and draft warrant, lodged with the court. The officer applying for the warrant, usually unaccompanied, attends before the magistrate in private at the appointed time to present the application. If there is a need for a more senior or experienced officer to accompany the applicant officer for assistance that will occur.

Police procedure leading to the court application is the same, a request for Technical Support resourcing (TSS) is made and, if approved, the outline of the extent of the surveillance operation, without technical detail and disclosure of methods, is provided by the TSS operative to the detective, who will then prepare the application, affidavit in support and the draft warrant, and make the appointment with the magistrate through court administration.

I have previously referred to the exchanges between investigator and technical support, and explained their roles, but it is important to understand not only the relationship between CIB officers and police officers operating within Technical Support, but also the exchange of information which occurs during this meeting/briefing. TSS operates in technical support of investigations but has no investigative role. The information on the technology and methodology TSS will utilise in installing and operating surveillance devices is not disclosed to investigators, I have previously explained the reasons for this. I consider those reasons to be valid. But the separation of roles and limits imposed on exchanges of information limit the level of understanding detectives will have, after that briefing, as to exactly how the surveillance device installation and operation will be achieved.

The application, affidavit and draft warrant will be drawn on the detective's understanding of where the targeted meeting(s) and discussion(s) are likely to take place, whether the discussions will occur over time and the likelihood that other people will be present or their conversations will be overheard and or recorded. In that affidavit the detective, 'the applicant' will include detail in a section headed 'Privacy.' The template available for use commences with the sentence: "The matters relevant to how much the privacy of any person is likely to be affected by the issue of surveillance device warrant are set out below." What follows that introductory statement will be the detective's understanding and assurances which the magistrate will rely on to state, in the warrant in para 5 (b) "In issuing this warrant, I have had regard to the extent to which the privacy of any person is likely to be affected." Justice Brett referred to the same introductory sentence in his second decision in the Thompson case which is referred to on page 34 of this report.

The detail provided by the applicant in this section of the affidavit, based on a limited understanding of the methodology and technology, will not, using the Thompson/Gleeson surveillance device experience, provide detail of the recording/surveillance technology and functioning, or any continuing recording in a professional or any other meeting room, if that officer does not have that information.

The Privacy section of the affidavit, coupled with any conditions in the warrant will be examined in my consideration of each of the matters when commenting on the adequacy of information provided to magistrates.

After completing the documents the applicant/detective will contact the magistrates court, seeking an appointment to have the application heard.

Of the 16 officers I interviewed, who had applied for the 19 warrants, I concluded that their experience with the time given for an appointment with the magistrate was similar. In all cases, bearing in mind there were no 'urgent' applications, the appointment given provided sufficient time (usually overnight) for the magistrate to read the application and accompanying documents before the hearing. The documents were, in some cases, transmitted to the court electronically. I believe that all documents are now electronically transmitted to the court.

I found that the training and experience of the 16 officers varied. Two officers had retired since their involvement. They were both very experienced and familiar with the requirements of the Act. All officers had an understanding of what was required, had available to them the templates and details for completion, some had received specific instruction in the requirements and processes for making an application for a warrant during training at the Academy. More senior or experienced officers had also provided assistance and mentoring and most officers had already applied for and obtained

Listening Device warrants under that legislation or surveillance device warrants under the Act. Their experience of other applications under the Act had, in most cases, been for installations in homes, vehicles and other 'premises' where considerations of secrecy and privacy are different to those applying in certain areas of a prison where, for example, in professional meeting rooms, changing uses, personnel and levels of confidentiality will occur.

The documents I examined were in keeping with the level of experience or training which the officers had and the support provided to them. Telephone intercept warrants were a common experience as well, but the legislation is federal and the process therefore jurisdictionally different. But, as indicated, precedents from earlier matters were readily available, as were the templates through office digital resources.

Not all officers had attended formal classes, or courses, for instruction focussed on the Act and its requirements and I will be making a recommendation concerning this fact and its relevance to the Terms of Reference for the Review.

I have examined all warrants and the accompanying application and affidavit on a number of occasions. Each time with a different focus. The first occasion followed my consideration of the decisions of Justice Brett in the Thompson case. I spoke with a number of concerned legal practitioners and then reviewed the files before interviewing the 16 officers and speaking with TSS officers. I also considered material provided by the 16 officers to Assistant Commissioner Blackwood in response to a request for responses to an extensive questionnaire covering aspects of the matters I had to review. The content of that questionnaire was settled with me by Assistant Commissioner Blackwood at the commencement of my Review.

The order in which I then approached the questions which required answering was to consider whether the warrants were valid on their face and then whether the mandatory requirements for the issuing magistrate were capable of being satisfied on the material provided in the affidavits. My answers to each of these questions follow:-

VALIDITY OF THE WARRANTS ON THEIR FACE.

Of the 19 warrants 4 were invalid on their face. All 4 warrants were sought by the Operation Ransack 2 team, and the invalidity was the same in every case. The warrant which Justice Brett considered in the Thompson case was the fourth and last Ransack 2 surveillance device warrant for prison premises. All four have the same flaw, describing the crime as "Conspiracy contrary to section 297(2)" in para. 3 of the warrant. All four were issued by the same magistrate in Hobart.

The flaw contained in the first warrant was repeated when the papers for the second and third warrants were being prepared by the officer who applied for the first warrant. The fourth warrant,

the one ruled invalid by Justice Brett, was applied for by another member of the Ransack 2 team. In all 3 subsequent warrant applications that first warrant appears to have been used as a precedent.

The details of the date of application, and issue and the prisons for those four warrants are as follows:-

Date on the application.	Date of issue.	Premises.
9/5/2017	9/5/2017	Women's Prison
11/5/2017	11/5/2017	Women's Prison
19/5/2017	19/5/2017	Women's Prison
13/6/2017	13/6/2017	Risdon Men's Prison.

The context for the warrant applications is best understood by recalling the background outlined on page 33 of this Report. When police became aware of a proposed meeting between Mclaren and Keefe on May 11, 2017, the first warrant, for the installation for a surveillance device to record the meeting was obtained.

The second warrant, applied for on the morning of May 11, was sought when police were informed, on May 10, of a proposed meeting, also at the Women's Prison on May 11, between Neill-Fraser and Ash and a well known Melbourne QC, who had travelled to Hobart from Melbourne with McLaren.

On learning of this additional meeting investigators, quite appropriately, first sought clarification from the Office of the DPP of any known professional relationship between the QC and Neill-Fraser. The affidavit in support of the application for the second warrant noted that the DPP's office had informed police on the afternoon of May 10 that "as far as the office was aware, neither Ash nor the QC were representing Neill-Fraser in her pending appeal". The warrant was issued at 9.30 on the morning of May 11 and the meeting took place later that day.

The first warrant did not result in any actual surveillance because the meeting which it was sought for did not take place. The second meeting took place and investigators later reported that the QC was not at that time acting for Neill-Fraser. The first warrant was obtained for the Keefe/McLaren meeting and the second for the Neill-Fraser/Ash, Melbourne QC meeting. With ongoing visits to both Keefe and Neill-Fraser a third warrant was sought and obtained on May 19 which authorised the installation of 'listening device(s)' in "visitor meeting rooms at the Mary Hutchinson Women's Prison at the Risdon Prison Complex" in respect of "conversations … of Karen Patricia Nancy Keefe and Susan Blyth Neill-Fraser and any visitors they may have". This warrant was the subject of an application for an extension, heard on August 1st and the device(s) retrieved on 24 August 2017. I will consider these warrants again under different headings, but the third warrant in some detail, which is why I have provided particulars to this extent.

The crime under investigation was correctly described as conspiracy in all the applications, but the use of "section 297(2)" is the flaw which renders the first three warrants invalid on their face. Reliance on a precedent is understandable, with a successful application for the first warrant, and an affidavit requiring evidence and detail of the same matters for the second and third affidavits. However, caution ought to have prevailed both at an officer and magistrate level. I will be making a recommendation concerning the use of precedents.

As indicated previously, the same error was also repeated in the fourth draft warrant, again caused by using the precedent. The affidavit in support of a warrant for the Thompson and Gleeson meetings relied on use of the lengthy outline of the evidence from the affidavits used in the first three applications, but the targets and suspects within the conspiracy were different. The affidavit for the third warrant was 32 pages long, the affidavit for this fourth warrant was 51 pages long, and paragraphs containing the reference to 'section 297(2)', referred to above, were not repeated in this affidavit.

All remaining 15 warrants were valid on their face. However, as stated earlier, I propose to go behind each warrant to examine the terms of all the warrants, the adequacy of the information provided to the issuing officers, the adequacy of any conditions or limitations imposed to mitigate the risk of capturing private conversations and compliance by Tasmania Police with any conditions and limitations, as required in paras. 2, 3 and 4 of the Terms of Reference.

REASONABLE GROUNDS FOR THE SUSPICION OR BELIEF FOUNDING THE APPLICATION.

Under s. 9 of the Act a law enforcement officer may apply for the issue of a warrant if that officer believes on reasonable grounds that a relevant offence has been, is being or is about to be committed, that an investigation is being, will be or is likely to be conducted in this jurisdiction and that the use of a surveillance device is or will be necessary in the course of the investigation. (s. 9(1)(a)(b) and (c)).

The magistrate hearing the application "may" issue the warrant if "satisfied that there are reasonable grounds founding the application for the warrant", referring back to the requirements of section 9. (see s. 11(1)

In the Thompson case Justice Brett had to consider this question and, as detailed earlier in this report, found on the affidavit evidence provided to the magistrate that there was sufficient detail and evidence provided to so satisfy the magistrate.

I have examined each of the affidavits for the 19 warrant applications (one being the affidavit in the Thompson matter) and I am satisfied that the officers who swore those affidavits provided sufficient evidence and detail for the magistrates to be satisfied that there were reasonable grounds for the suspicion or belief to found the application for each warrant.

THE REQUIREMENTS OF SECTION 11(2) OF THE ACT.

S. 11(2) of the Act contains details of what the magistrate MUST have regard to when determining whether a surveillance device warrant should issue. There are 5 matters which the magistrate must have regard to and they are listed in para 5 (a-e) of the warrant. Every affidavit in support of the applications for the 19 warrants addressed these issues and because one of them, privacy, is central to paragraphs 2, 3 and 4 of the Terms of Reference I will attend separately to that issue. I will address the other 4 questions collectively and return to the question of privacy.

'Section 11(2)

In determining whether a surveillance device should be issued , the magistrate must have regard to:-

(a) The nature and seriousness of the alleged offence in respect of which the warrant is sought;
(b) The extent to which the privacy of any person is likely to be affected;
(c) The existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation;
(d) The evidentiary or intelligence value of any information sought to be obtained;
(e) Any previous warrant sought or issued under this Division, a corresponding law etc…."

I found that the requirements of s. 11(2)(a)(c) and(d) were all satisfied by the detail provided in the 19 affidavits. I was not able to independently verify the accuracy of the detail provided to satisfy the requirements of s. 11(2)(e), for those matters where detail of other warrants was provided, but in every affidavit a separate, headed section, addressed this question, either in the affirmative, with particulars, or negative, and as I had earlier tested the information provided by retrieving those two additional files I determined to accept what was in the affidavits.

I am satisfied therefore that all 19 affidavits provided the magistrates with material upon which they could be satisfied that the 5th requirement in s. 11(2) had been complied with.

PRIVACY, PRIVATE CONVERSATIONS AND SURVEILLANCE DEVICES IN A PRISON

The issue of privacy is complicated by the kinds of warrant available. The warrant application forms permit the issue of three kinds of surveillance device warrant, (see s. 13(1) and attachment 'B'). A 'specified premises' warrant, a 'specified object' warrant and a 'specified person' warrant. A warrant may authorise the installation of devices for all three kinds of warrant but of the 19 warrants applied for only one application contains a request for an 'objects' warrant, which is not repeated in the warrant which was issued. I have assumed that this was a typing error as the person who completed the form for the application also completed the draft warrant submitted to the magistrate.

18 of the applications are for specified premises warrants and 11 also seek the issue of a 'persons and conversations' warrant.

With few exceptions the applications seek warrants for the maximum statutory period, 90 days. I understand this, as a matter of precaution it will avoid the need to seek an extension or a fresh warrant. A warrant for a 90 day period is more appropriate where the warrant is sought for private premises and situations where there is no pre- determined appointment or meeting time, unlike most of the situations within a prison. However, a warrant issued in broad terms, when the affidavit suggested a narrower focus, permits a widening of focus if change is encountered in the term of the warrant.

The applications for premises warrants permit a breadth of warrant which, without requiring identification of a person, allows a similar breadth for surveillance. But the Act does permit the issue of warrants in broad terms, a fact noted by Justice Brett in The State of Tasmania v. Jeffrey Ian Thompson No 53/2022:

"provided that the warrant is within the terms of the legislation, there is no reason why it cannot be extremely wide, but the person reading the warrant needs to understand that."

I will comment on this in due course but, as mentioned, an important communication in the process of issuing a warrant is the briefing between the investigator and the TSS officer when discussing the outcome to be achieved from the surveillance operation. The next important communication is through the affidavit and other documents presented to the magistrate. The application must point to the type of surveillance exercise which is anticipated following discussions between investigator and technician and this must be supported by the accompanying affidavit so that the magistrate is provided with evidence supporting the issue of the warrant and any conditions concerning privacy.

PRIVACY

Privacy is not defined in the Act, yet the issuing officer MUST have regard to "the extent to which the privacy of any person is likely to be affected" by the issue of the warrant. (s. 11(2)).

'Private conversation' is defined in the Act to have 'the same meaning as in the Listening Devices Act 1991', which definition I referred to on page 8, to mean "any words spoken by one person to another person or to other persons in circumstances that may reasonably be taken to indicate that any of those persons desires the words to be listened to only by themselves or by themselves and by some other person who has the consent, express or implied, of all persons to do so."

The terms of reference relevant to this aspect of my Review (pars. 2,3 and 4) use the term "private conversations unrelated to the investigation in respect of which the warrant was sought."

With few exceptions, and the Gleeson/Thompson warrant is one of three, the warrants only sought approval for the use of 'listening devices,' not optical surveillance. That is likely to be the consequence of a combination of :-

(i) the 'what is required' briefing between the detective and TSS officer, supported by
(ii) the fact that all 19 subsequent affidavits attest to a desire to record or capture conversations between the target of the exercise and a visitor or visitors'
(iii) a prison environment where most prisoners are under some form of visual scrutiny anyway.
(iv) if other persons, outside the investigation, are present in a visitor area there is an assumption that there is no sense of visual privacy in the sense conveyed by the definition.

I propose therefore to confine considerations of privacy to private conversations referred to in the Terms of Reference and as defined in the Act.

THE BREADTH OF THE WARRANTS APPLIED FOR AND ISSUED.

I have previously referred to the three 'kinds' of warrant :-

(i) the warrant of a kind referred to in s. 13 (1)(a), a 'specified premises' warrant
(ii) the warrant of a kind referred to in s. 13(1)(b), a 'specified object' warrant
(iii) and warrant of a kind referred to in s. 13(1)(c), a 'specified persons' warrant

There are no specified object warrants in the 19 matters under review. A consideration of the breadth of the warrants issued requires an examination of what each of the remaining kinds of warrant authorises.

1. The specified premises warrant, when issued without conditions, authorises the installation of surveillance devices on the specified premises, which can be described widely. Descriptions such as "Her Majesty's Prison Risdon", "within a visitor meeting room at the Risdon Prison at 672 East Derwent Highway, Risdon Vale", or "Launceston Reception Prison, Cimitiere Street, Launceston" are used in the warrants I have examined, and there are others. A specified premises warrant is not required to identify the person who is the target of the surveillance operation. The assumption on the part of an issuing magistrate will be, supported by the material in the affidavit, that the target of the covert surveillance is a named prisoner or person on remand. There is nothing in the Act which provides any clarification or qualification to the breadth of a warrant issued in those terms. If the warrant is issued without conditions it becomes a very broad warrant. I had expected to see more 'premises' warrants with conditions.

2. A specified persons warrant has a similar breadth, but is limited by the focus of the warrant on that person. A specified person warrant does not have to identify, on its face, any premises. The Act provides for that, in s. 13(2)(c)

" A surveillance device warrant authorises, for a warrant of a kind referred to in subsection (1)(c) (a specified person warrant) (i) the installation, use and maintenance of a surveillance device of the kind specified in the warrant, on premises where the person is reasonably believed to be or likely to be; and(ii) the entry, by force if necessary, onto the premises referred to in subparagraph (i) or subsection(3)"

All 19 warrants examined contain authorisations for specified premises and 14 of those warrants also specified a person or persons as the target of the warrant, resulting in a warrant authorising the use of a surveillance device for specified premises and for the conversations and movement of a specified person or persons, which is permitted under the Act.

The affidavits in support of all 19 warrants identified a meeting or occasion with the anticipation of a conversation or conversations, involving an identified person, the target of the proposed covert operation. The privacy section of every affidavit advised the magistrate, in varying degrees, of the extent to which the privacy of any person was likely to be affected by the issue of the warrant.

While the bulk of the affidavit contains information supporting the evidentiary basis for the application and may appear to be directed towards matters other than the privacy of 'any person,' that information has a broader purpose.

I have examined the matters which the issuing magistrate must consider in determining the application (s. 11) :-

(1)(i) if the magistrate is satisfied that there are reasonable grounds for the suspicion or belief founding the application the magistrate may issue the warrant but, in determining whether to issue the warrant, the magistrate must have regard to:-

(2)(a) the nature and seriousness of the offence,

(b) the extent to which the privacy of any person is likely to be affected

(c) the existence of alternative means of obtaining the evidence

(d) the evidentiary or intelligence value of any information sought, and

(e) any previous warrant sought or issued under this Division.

The matters which the magistrate is required to have regard to provide a guide to the weighing and balancing which must occur. Weighing the case, the investigation, the seriousness of the suspected offending, what may be gained from the exercise and, taking those matters in to account, balancing them against the interests of and likely affect upon any person's privacy and whether an authorisation to use covert surveillance on someone should be given.

The magistrate is required to have regard to the 'extent' to which the privacy of any person is likely to be affected, not refuse the application if there is any prospect at all that a person's privacy is likely to be affected. It is the 'extent' to which it is likely to be affected. The issue becomes a balancing of interests and protections.

Therefore the premises on/in which the surveillance device is proposed to be installed, the use to which those premises will be put, the persons present or likely to be present when any recording will occur and the nature of any activity occurring in the vicinity of the device become important considerations for the applicant and the issuing magistrate. Those considerations will change with the premises. The home or residence of a surveillance target is different to visiting and meeting areas in a prison.

For example, the location of the Thompson/Gleeson listening devices, which were recording continuously, in a professional meeting room. The likelihood that highly confidential/ private conversations would be held in that room was real. That was a matter which should, if known, have been disclosed to the magistrate so that it could be placed in the balance. I am satisfied that the officer who swore that affidavit did not know that continuous recording would happen. Should the application be refused or conditions imposed on the execution of the warrant which will limit the use of any device when the target is not in the room? Should the deponent of the affidavit have a better understanding of what is to occur?

If on the other hand the targeted conversation is to occur in a place which is isolated or semi-private, within view of prison officers, but out of hearing and the surveillance/recording will be confined to the location of the meeting or visit. Are conditions required if the legislation permits a broad warrant and the explanation in the affidavit of the likely affect on any other person's privacy refers to the risk of peripheral or background conversation recording?

Using another example of a prison facility. One of the visiting facilities at the Risdon Prison is a large room with tables and chairs placed around the room for multiple prisoners to have contemporaneous contact visits in that room. Conversation can be heard and prison officers can be present in that room, hearing, and seeing the interaction. Will the installation of a surveillance device in that room, aimed at capturing a particular prisoner's conversation with visitors which records for a sustained period so affect the privacy of other persons in that room that either a warrant be refused or conditions imposed which render the exercise futile?

Will a conversation between a prisoner, the target of a surveillance operation, and a visitor taking place in close proximity to another conversation, in similar circumstances, which is likely to be picked up and recorded by the device at the same time, be a sufficient risk to refuse the application for a warrant or, in balancing the interests, should the over recording be 'regarded' as an acceptable risk if the crime under investigation is murder?

I must evaluate issues such as this because I am required to consider the adequacy of information provided to issuing officers (Term of Reference 2) and the adequacy of any terms and conditions imposed (Term of Reference 3) in the 19 applications under consideration.

The term "private conversations", as defined and used in the Terms of reference is the right yardstick to apply to these matters when I consider them in the settings in which the surveillance devices were installed.

I outlined at the start of this section the details of the Terms of Reference which require me to consider, amongst other things, the adequacy of information provided to issuing officers in surveillance device warrant applications in relation to the risk of the device capturing private conversations unrelated to the investigation and any proposed measures to mitigate the risk of capturing such private conversations. I will deal with this requirement separately for reasons which will become obvious.

THE ADEQUACY OF INFORMATION PROVIDED TO ISSUING OFFICERS.

2(i). Relating to the Risk of Capturing Private Conversations unrelated to the investigation.

I have closely examined all 19 matters from the perspective of the proposed location, meeting/visiting facilities or room and the likelihood of other persons being present, as outlined in the affidavit accompanying the application and any assurances given in the affidavit for the avoidance of capturing private conversations. I will divide the matters in to two lots. One of 15 and the other of 4.

I consider that 15 of the 19 matters concerned applications and affidavits where adequate information was provided to the magistrates in relation to the risk of the use of the surveillance device capturing private conversations unrelated to the investigation in respect of which the warrant was sought. In all 15 affidavits there was a degree of confidence that the recording from the device would be focussed and there was little or no risk of capturing other content and, in one matter, if it was, the risk was minor and the seriousness off the offence under investigation in effect weighed in favour of the risk.

Three of the meetings did not take place and the other 12 resulted in a discrete or achieved recording of the conversation being obtained without capture of any private conversations.

2(ii). Proposed Measures to Mitigate the Risk of Capturing Private Conversations unrelated to the investigation.

In the 15 matters under consideration, to summarise, the only proposed measures within the affidavit, related to the location and timing of the meeting or meetings, mitigations such as details of the nature of the facility where the meeting would take place, the likelihood of other persons being present or nearby and their conversations being recorded as well as the nature of those meetings gave a measure of assurance that the risk of capture of private conversations was mitigated. No disclosure of the technology or methodology or duration of recording was contained in any of the affidavits in support.

3.ADEQUACY OF CONDITIONS IMPOSED BY ISSUING OFFICERS.

I am to consider the adequacy of any conditions or limitations imposed by issuing officers. Only one of the 15 matters involved the issue of a warrant with specific conditions. That warrant was issued in Launceston and the meeting, for which the warrant was sought, did not take place. I have commented on this warrant to the officer to whom it was issued when I interviewed him. The condition imposed on the use of the device is in my view more than sufficient to mitigate the risk of capturing other private conversations. The meeting was to take place in Launceston, where the facilities permitted discrete recording.

The draft warrant taken to the magistrate in this matter was for both specified premises (Launceston Reception Centre- Cimitiere Street, Launceston) and a specified person, a named inmate. The condition to which use of the surveillance device was subject (para11 of the warrant) was expressed in these terms “The surveillance device may be used subject to the following conditions: It is to be used to listen to and record conversations of XXX (the named inmate) only”.

That condition is typed and the applicant officer, when I interviewed him, almost 5 years after the event, said that he believed that the magistrate had entered that condition or asked him to do it, he was not certain which.

The remaining 14 matters all involve the issue of a warrant without specific para. 11 conditions.

4. CONSIDER COMPLIANCE BY TASMANIA POLICE WITH ANY CONDITIONS OR LIMITATIONS IN 3.

There were no conditions. Of the 15 matters 6 were specified premises only warrants, all without conditions and 9 were specified persons and specified premises warrants, combined, also all without para. 11 conditions

I will comment about this when I conclude my examination of the remaining 4 matters, which I will do individually. The absence of para. 11 conditions from all but one of the warrants is a matter about which I have speculated since the early days of this Review.

THE FOUR REMAINING WARRANTS FOR CONSIDERATION.

Warrant 1 Issued on 19 May 2017.

When considering this matter I will refer to the two people who were the target of this surveillance operation and some others also mentioned in the documents. They have been referred to at length in the second matter I will deal with under this heading and there is a coexistence between matters. The remaining two matters I will treat anonymously, court proceedings may not have resulted and I would prefer to deal with the matters in this way.

This warrant was the third warrant applied for with the reference to section 297(2) of the Criminal Code which Justice Brett later held was an invalidity on the face of the warrant and followed those earlier warrants. I provided detail of the warrant and application on page 50.

The warrant issued for 90 days and was both a specified premises warrant ("visitor meeting rooms at the Mary Hutchinson Women's Prison, Risdon Prison Complex") and a specified persons' warrant ("Karen Patricia Nancy Keefe and Susan Blyth Neill-Fraser and any visitors they may have")

On 1 August 2017 an application was made to extend the term of the warrant and to extend the warrant to cover the Launceston Reception Centre, as it was understood Keefe may be moved there. The extension application was granted and the devices, already installed, were removed on 24 August 2017.

Privacy.

This warrant was included in the summary in which I referred to the sufficiency of the evidence disclosed to the issuing magistrates in support of the applications for all 19 warrants. I will not reconsider the sufficiency of that material.

The section of the affidavit covering the issue of Privacy followed a description of the investigation to that stage and the need to gather further evidence, particularly with the number of visits to the prison, to determine the extent of involvement of the two named persons and other people in the suspected conspiracy to pervert justice. The "any visitors" addition to the specified persons aspect of the warrant (above) is explained.

There is an assurance that the privacy of persons other than five named persons (including Keefe and Neill-Fraser) "would not be unduly interfered with" followed by the following assurance:-

"(a) Police can obtain information relating to times and dates of relevant meetings and can isolate the monitoring of any listening device product to meetings relevant to this investigation. Therefore any personal or legal visits between inmates and visitors not directly involved in this investigation will not be monitored."

"(b) Police do not intend to monitor visits that obviously only relate to professional legal visits involving Neill-Fraser's Appeal"

"(c) If the proposed listening device does capture incidental conversations relating to Neill-Fraser's appeal, personal or legal conversations involving Keefe or conversations involving people not involved in this investigation the seriousness of what is being investigated would outweigh the possibility of capturing those conversations."

I have listed this matter in the 4 matters I wish to examine separately because although the warrant which was issued did not contain any specific para. 11 conditions it did identify the conversations it authorised surveillance of (page 50) and, as the surveillance exercise continued the nature of the recording process was altered. The matter therefore requires mention because of the questions I am required to consider under the terms of reference.

Under the warrant recording commenced on 19 May. Individual and identified meeting recordings were occurring both in the professional meeting room and in the contact visitor area, using two separate devices which the warrant authorised. Downloads from those devices occurred on May 22, 27 and 29, June 5, 12, 13 and 19. At about this time the notification of meetings from the prison office was becoming irregular and some meetings were missed. Additionally, TSS was then conducting three operations at the prison and the covert nature of the work was at risk of exposure due to the increased attendance of TSS officers at the prison. (Some of the detail of this was provided to Justice Brett during the voir dire). On 27 June the recording in the professional meeting room at the women's prison continued as before, recording individual and identified meetings, however a continuously recording device was set in the contact visitor facility to record from 8.30 – 4.30 each day. The surveillance operation continued this way until the devices were removed.

In my view there is a distinction between the 'privacy' of conversations held in a contact visitor area and those conducted in a professional meeting room. Proceedings against Keefe were discontinued following the ruling in the Thompson case and the question of admissibility was not tested at trial. I have considered all the circumstances and believe that they are distinguishable from those in Thompson's case and that any relevant material recorded on the device in the contact visitor facility would be admitted under s. 138 of the Evidence Act, where I believe the discretion would, on balance, be exercised in favour of admission. The warrant would be held invalid on its face and the prosecution would then carry the onus on the question of the exercise of discretion to admit under s. 138. I understand that the discontinuance of the Keefe prosecution was not referable to the question of validity of the warrant but other good and valid reasons for exercising the prosecutorial discretion were taken in to account.

Warrant 1 and the TERMS OF REFERENCE.

TOR 2(i) I consider that the information provided to the magistrate at the time of the application was adequate in light of the surveillance processes being followed and:-

2(ii) the proposed measures were, at the time, also adequate.

BUT, when it was determined by TSS to change the recording regime and instal a constantly recording device in the contact visitor area a decision should have been made to refer the matter back to the issuing magistrate for variation, which would give the magistrate the opportunity to either vary the warrant or decline to allow the continuation of the surveillance in the contact visitor area.

The issue of a 90day warrant provides opportunity, with time, to consider variation of approach and I will return to consider this after examining the remaining matters.

TOR 3. The adequacy of conditions or limitations imposed.

As there weren't any conditions imposed and, the final result may suggest that the conditions while adequate to start were later not adequate for what then transpired. The 'limitation, for this 'specified persons' warrant, was adequate.

TOR 4. Compliance by Tasmania Police.

The conduct of Tasmania Police was in accordance with the warrant issued however, internal procedures (measures taken) by TSS and examined earlier in relation to the Thompson matter while not preventing capture of 'any' private conversations which may have taken place in the contact visitor area, the product would not have been retained or had access permitted to that product by any detectives before deletion or erasure. For the reasons outlined after my examination of the Thompson matter, the problem was that the magistrate should have been made aware of what was happening to be given the opportunity to decide, knowing what the facts, or changed facts were. The matter should be settled at that stage and not left to the discretion of a trial Judge.

The separation/confidentiality between investigators and TSS was scrutinised in the Thompson case. At one stage during the voir dire, when the TSS officer was being questioned by Justice Brett, the following exchange occurred

HIS HONOUR: "So you just left it – you didn't do that, you left it running indefinitely, and why did you do that? Why did you leave it running indefinitely?"

WITNESS: "Just, just because the – being able to switch it back on and off remotely wasn't always a given because technical issues do occur, and it was in the knowledge that I would only extract the parts that were applicable to the meetings that took place – or the meeting that took place. Anything else wouldn't be accessed, or viewed, or downloaded."

It became apparent to me while interviewing detectives and TSS officers that the refusal by TSS to disclose technology and methods to detectives and to not allow access to recording equipment could create the sense that their technological oversight in cases where the "extraction of the parts that were applicable" provides an "own volition" measure of mitigation as raised in TOR 4. While that may very well be the case, for the reason given, this is something which should be disclosed to the magistrate at the time the warrant is applied for or when changed conditions arise during the term of the warrant. With this warrant the opportunity also arose when the extension was sought. However, as I have said, I believe the s. 138 discretion would favour admission.

WARRANT 2. ISSUED ON 13 June 2017

This is the warrant which Justice Brett ruled invalid and there has been adequate examination of the warrant and the circumstances of its execution. His Honour's conclusion that the magistrate should have been informed that the constant recording on the devices in the professional meeting room would occur, in a sense, will support my recommendations arising from these four matters.

WARRANT 3.

The application for this warrant sought a specified premises authorisation with the nominated premises "within a visiting room at the Risdon Prison at 672 East Derwent Highway, Risdon Vale, Tasmania." The devices authorised under the warrant were a listening device and an optical surveillance device.

A specified person authorisation was not sought, and no conditions were imposed in the warrant. However, within the affidavit in support of the application the warrant sought it is clear that the purpose of the warrant was the attempted capture of conversations between a known inmate and visitors. The warrant was subsequently extended in time without inclusion of any conditions.

The purpose for this surveillance operation was to endeavour to record conversations with the target inmate in a large contact visitor meeting room at Risdon Prison. The recording was downloaded each day but the device was ultimately retrieved because multiple conversations were causing poor recording. When I interviewed both the detective applicant and a senior officer from TSS about this matter I formed the view that this warrant did not involve the recording of 'private conversations,' as defined, should any untargeted conversations be captured in that environment because of the nature and use of the premises.

The reason why I have included this matter for consideration is that the affidavit does not state specifically that the devices would constantly record in the area in which they were to be installed. Would the magistrate, if informed of that, have required conditions?

TOR 2(i) adequacy of information to issuing officer as to the risk of the surveillance device capturing private conversations. I have concluded that the location of this surveillance device was where the conversations capable of being recorded were more than likely not private conversations, and the privacy assurance/information in the affidavit was adequate.

TOR 2(ii) the proposed measures for mitigating the risk of capture as outlined in the affidavit were adequate.

3.There were no specific conditions imposed on the warrant.

4. There were no conditions to comply with and the process of managing recorded product by TSS, in the circumstances, was adequate.

Warrant 4

This warrant was sought to approve the installation of a surveillance device in the Launceston Reception Centre. The warrant sought was both a specified premises warrant and a two specified persons warrant. No other conditions were imposed on the warrant. It was issued for 90 days.

The crime under investigation was a very serious one and I will endeavour to maintain a level of anonymity in the way in which I report my findings.

The surveillance operation was the proposed installation of a listening device in the Reception Centre in an attempt to capture the conversations between two co offenders who were being held in the centre. The device was set to constantly record, which it did for four weeks.

Privacy

The affidavit in support of the application informed the magistrate that the device would be placed within the Reception Centre where the two inmates would be residing “in order to gain information of the crime.” “Other persons work and reside at that address, however, having regard to the seriousness of this matter, any breach of those persons privacy is considered necessary.” And then:- “Any incidental interference with the privacy of any person would be justified given the seriousness of the matter under investigation.”

The listening device installed in the Centre recorded constantly for 4 weeks.

I have examined the affidavit carefully and while there is no mention of the device continuously recording the description of the recording operation in the affidavit, the nature of the use of the area in which the device would be located, coupled with the strong submission concerning the balance tipping in favour of recording over privacy, satisfies me that the magistrate was readily able to be satisfied of the issues of privacy and settle in favour of issuing the specified person warrant without other conditions.

The magistrate who heard this application 5 months later imposed the condition in the warrant which I mentioned earlier. The only warrant of the 19 with any specific condition.

TOR 2(i) Although the applicant did not state that the device would be set to continuously record, I consider that the information provided to the magistrate was adequate. A device set in a centre to record conversation of two residents does not compare to a device in a professional meeting room, or a private part of the Centre.

2(ii) There were no proposed measures to mitigate. I have set out the text of the affidavit relevant to assurances and information concerning privacy.

TOR 3. There were no specific conditions.

TOR 4. There were no conditions to comply with nor were there any self-imposed measures.

CONCLUSION TOR 2,3 and 4.

That concludes the report of my examination of the adequacy of information provided, the content of and compliance with any conditions imposed on the warrants which were issued during the period under review. I have gone behind the face of each warrant and that has enabled me to identify three further warrants where I consider that more information may have been provided to the issuing magistrate either at application or, because of changes to the surveillance methodology, during the life of the warrant. In one other matter, Thompson, which I have considered at length, the continuous recording in a professional meeting room should have been disclosed.

I have identified the comparative differences between the locations or use of the areas in which the other three surveillance operations were being conducted and the professional meeting room in Thompson and concluded, on balance, that a court would, in those three matters, exercise its discretion and admit the surveillance evidence under the 'Bunning and Cross' discretion (s 138 of the Evidence Act).

The tightly held knowledge or confidentiality of technology and methodology in the operational activities of detectives and TSS officers, which I understand (I have given assurances based upon it) and would not seek to overturn in this Review may create a high degree of confidence within the ranks, akin to "adequate measures taken by Tasmania Police of its own volition to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations." (see TOR 4 and my comments on pp 61 and 62). The use of a continuously recording device which may result in the capture of other, unrelated, conversations which will not be monitored or disclosed because they will, when accessed by the technical expert who has exclusive operational oversight of and access to it, be erased, will not be seen by an issuing officer, Judge or magistrate, as a fact which ought not be disclosed in consideration of privacy implications at application.

ACKNOWLEDGEMENT

Before moving to the remaining items in the Terms of Reference I wish to record my appreciation for the level of cooperation I received from all officers from Tasmania Police who attended at my request and answered all questions asked and assisted when I asked for assistance. Any recommendations and the commentary which precedes them should be seen, in part, as a result of that cooperation and the willingness to contribute and learn from the exercise which they all demonstrated.

TOR 5. IDENTIFY ANY IMPROVEMENTS IN APPLICATIONS FOR WARRANTS.

I will, as mentioned, be making comments outside the scope of the Review Terms of Reference, but those comments tie in with suggestions I will make about improvements to the process as required under the Terms of Reference.

Some of what I will say has already been addressed through the internal review which I was informed of at the time of my appointment and I will comment to that effect when I address those points.

(a) Preparation of Documents.

I have attempted, with the detailed outline of the requirements of the Police Powers (Surveillance Devices) Act 2006 in this Report, to not only provide a basis for understanding the balance of the Report, but to demonstrate that the task of considering all aspects of an application for a surveillance device warrant for any premises and target is not simple and care should be taken in preparing the documents which must be lodged with the court.

I was prepared to recommend that the task of preparing the application, affidavit in support and the draft warrant be undertaken with some input from the Legal Services Division of Tasmania Police, aided by a set of templates and instructions which were user friendly. I am not saying that what was available before was a hinderance, but the available materials may have been challenging to the newcomer.
The advisory and oversight work undertaken by more senior officers is commendable, and I do think that assistance in checking the content and form of the documents by someone distanced from the front line of the investigation is helpful. The input of a qualified lawyer will add a layer of assurance to this process.

Internal Review.

I became aware at the commencement of the Review that an internal review had been commenced shortly after the decision of Justice Brett in the Thompson case and I was provided with an opportunity to consider the progress made (the internal review has been ongoing) when I had the time to do so.

In August 2022 operational changes were made to procedures for the execution of surveillance device warrants following a review into the "current procedures for the application, authorisation and implementation of warrants issued under the Act". The initial changes involved revamped administrative oversight through the Surveillance Services Coordinator and a requirement that the supporting affidavit application and draft warrant were to be signed by an officer of the rank of sergeant or above. (The rank of an applicant under the Listening Devices Act.)

Further, the Legal Services Division of Tasmania Police, since last year, has an oversight role in the settling of the application, affidavit and draft warrant. The folder of templates for use in applying for surveillance device warrants and accompanying instructions has also been updated by Legal Services, a task completed just recently. I have inspected the folder and it is more instructive and helpful than its predecessor, and it attends to many of the challenges of following a checklist of the legislative requirements.

Before I commenced the Review steps were taken to provide for a legal officer to accompany the applicant officer, not as an advocate, when the application is heard. The Chief Magistrate has confirmed that this process is now in place. I think this is also an improvement and will assist the applicant after the hearing should the magistrate raise amendments or issues.

(b) The Affidavit.
The exchange of information concerning technology and methodology passing from a TSS officer, who will execute the warrant if the magistrate issues it, creates what I have referred to as the first exchange of information. The applicant officer must provide the magistrate with assurances concerning privacy and that becomes a challenge because of the restrictions, for the reasons explained in the Report, on TSS officers' disclosure of methods and technology, and probably a reluctance to say more than is deemed necessary as a consequence. It is not a Tasmania only issue, as I will point out under Safeguards.
There will be ways to work through this which don't risk disclosure of protected information. If the task is not achievable without resort to the operation of a device which is continuously recording with privacy implications which will not be acceptable to the magistrate, so be it, but considerations of the type outlined in my commentary on Warrant 1 on page 56 are at least feasible. The two officers will have to evaluate what can be disclosed, and whether that provides the magistrate with sufficient evidence to determine the application, or assure privacy concerns with the imposition of conditions. If it wont fit, don't try.

(c) The Draft Warrant.

The applicant officer's presentation of documents to the magistrate is the second exchange of information in the process. The officer's affidavit and documentation should present the magistrate with a clear indication of what is being proposed and the evidence which supports the application. The 'hearing' is not the presentation of further submissions and argument, the proceedings are heard in the absence of another party and if the documents don't speak for themselves there is a problem. There are other requirements under the Act for retention of records, which will not provide an effective layer of scrutiny to the process if there is dialogue with the magistrate which adds evidence not recorded in the affidavit or reflected in the warrant. I was surprised by the high number of warrants which contained superfluous clauses and redundant sections. As mentioned in the Report, some can easily be deleted by the officer preparing the documents but others are the domain of the issuing magistrate or Judge.

All the officers I spoke with rightly regarded the sections 6(d), 11 and 12 on the template warrant as sections for the magistrate to complete.
I had anticipated specific conditions on some warrants, not as in a 'specified person' warrant, naming that person as the target of the surveillance operation.
If the position taken by some magistrates is that the draft warrant presented to them contains the desired terms and conditions for the warrant which the applicant seeks, and I am speculating here, then I think there is a risk that other magistrates will be confronted if presented with a draft warrant with conditions already drawn for the magistrate to adopt. It is not for the applicant officer to draft such conditions in the warrant, it is the task of the magistrate, after balancing the competing issues, to impose conditions, if any, which suit that outcome.

(d) The 'kind of Warrant'

The presentation of the issued warrant is the third exchange of information in the process. The terms of the warrant should enable the TSS officer, who receives it, to execute the warrant by installing the device(s) as authorised by the magistrate who issued the warrant.
I have outlined the differences between what a 'specified' premises warrant and a 'specified' person warrant authorise and the breadth which the former has, without conditions, particularly where the target is identified within the affidavit. I suggest that care be used when settling the form of the draft warrant to consider the benefit of seeking both a premises and person warrant.
6 of the 19 warrants, albeit 5 in the earlier years of the Review period, were premises only warrants. I asked some of the authors of those documents why they chose 'premises,' two replied that they thought you had to specify premises. (Which a 'specified person' warrant does not, as explained earlier in this Report).

It may be that the dialogue leading to engagement of TSS services concentrates on premises, which is understandable; but I suspect an applicant would also be concerned to identify the Prison to the issuing magistrate, which would not be necessary in a 'person' specified warrant. All that is speculative, but the choice should be considered with those points in mind.

(e) The duration of the warrant.

This is also something which needs to be considered. I was intrigued by the number of warrants with 90day maximum terms. Once again, as mentioned in the Report, a warrant with a 90day term is likely to be one issued for surveillance of a person not in detention, who does not have the restricted social interaction of an inmate. If the target, in custody, is meeting a visitor in 6 days, a 90day warrant may seem excessive, but the term of each warrant must be assessed to suit the circumstances.

(f) The checklist for legal compliance.

The description of the charge, and other issues, such as an explanation of the evidentiary value of the product expected from the surveillance operation are important. This task will be assisted by the oversight of members of the Legal Services Division.

(g) Avoid slavish reliance on precedents.

I realise that there is a need for precedents, but the technical slip in the Ransack 2 description was missed by two officers and a magistrate who read the documents 4 times. I understand that the Chief Magistrate has introduced an arrangement for the rotation of magistrates undertaking this administrative task. I think that is a very good outcome.

(h) If requirements of an operation change arise.

For example where constant recording becomes necessary to avoid the risk of disclosure of the identity of covert operatives, it is important to review the warrant and decide whether the conditions or limitations in the warrant permit that or require variation. Should the matter be returned to the magistrate? These decisions should be considered with advice and that advice followed.

(i) While, strictly speaking, not an application issue, I cannot leave this section without emphasising the importance of ensuring, through the checking process already applied, that the section 29 report is properly completed and signed off. This report is an important compliance document for the Inspection Entity.

(j) I was considering recommending a refocussed training model for refresh and training for existing detectives and inductees. The steps required for the completion of a full set of documents for a warrant application are not straight forward. Work was already being done on this and one of the officers I interviewed as a former applicant for a warrant was, at the time of interview, involved in preparing training at the Academy. Then the issue with the role of the Ombudsman, outlined under Safeguards (following), arrived and the solution of an additional training task presented itself. I support the steps being taken, they are explained further in the Safeguards section.

The finer issues which are picked up in pre hearing document review, process and oversight are all matters which will refine the work in this area and avoid error.

TOR 6. MEASURES TO MITIGATE RISK TO LEGAL PROFESSIONAL PRIVILEGE.

The last Term of reference requires me to consider any specific measures which may be required to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought which may be subject to legal professional privilege and to prevent access to, or retention of, any such conversations.

1. The risk of capturing conversations which are protected by legal professional privilege, particularly in the environment such as a professional meeting room within a prison, can be mitigated by the exercise of appropriate care and attention. Meeting rooms in which lawyers and their clients meet to discuss pending cases or other matters requiring legal advice should, with appropriate checking, be able to be avoided because of the booking or appointment necessary for such a meeting to take place.
2. The relationship of solicitor and client will not always be the reason for a lawyer meeting with a person in prison. That person may be a witness. In such cases there would not be the question of client professional privilege but the conversations would, if connected with the preparation of a client's case, involve issues requiring advice for detectives and disclosure around privacy issues if an application for a warrant is made after that advice.
3. If there are concerns that legal professional privilege may arise, or there are real risks that it will arise the prudent step must be to first take advice and, if continuing, detail those concerns in the affidavit in support of the warrant application, as suggested in 2. That may result in a refusal or the imposition of strict conditions.
4. Clearly there are risks once the surveillance involves a person in custody.
    a. Has that person been charged or is that person appealing a conviction and sentence? In both cases there is every likelihood that a solicitor visiting that person is there to give advice and take instructions. In such a case, particularly if a warrant is to be obtained, the prudent step would be to request that there be imposed a condition in the warrant that any recording device be turned off for the duration of the visit or meeting.
    b. Has the person's trial or appeal concluded and if so what is the purpose of the solicitor's visit? In such circumstances advice should be sought.
5. I have confined my comments to a very broad range of possibilities involving visits to people in custody where some notice of the visits is likely to be available. With surveillance devices installed in offices, homes and places frequented by a broad representation of community members a legal professional privilege situation may occur without notice/warning. I will not attempt to describe an acceptable list of scenarios. If anything like that occurs without warning, on discovery advice should be obtained immediately.

SAFEGUARDS

The Act provides safeguards or accountability measures for the processes I have been considering in this Report and I will examine them because people I have spoken to have raised concerns with me that those safeguards have not worked, "if they had there would not have been an adverse ruling in the Thompson case."

The case has highlighted a need to review and reset and I am grateful to the people involved in the case who have been willing to contribute to the dialogue concerning the issues which I have examined.

The safeguards within the Act are:-

1. The warrant must be issued by a magistrate or Judge before the surveillance can begin and the warrant application must be supported by an affidavit.
2. The officer who applies for the warrant must report back to the Judge or magistrate who issued it within the time specified in the warrant under s. 29 of the Act. That report,(I have attached a copy of the template to the Report 'C') requires the provision of considerable detail on the use of the powers under the warrant and includes reporting on the benefit to the investigation of the use of the surveillance device.
3. The Act imposes strict conditions on the use, disclosure and communication of protected information. (for which an exemption by amendment of the Act was obtained for this Review and publication of a Report)
4. The retention of records, or record keeping obligations, imposed on the Chief Officer of the law enforcement agency are well defined in the Act. (ss. 37, 38 and 39). These records establish a paper trail for compliance inspections which must be undertaken annually and reported on by the Inspection Entity under ss. 41 and 42 to the Minister. That report is tabled in Parliament. In Tasmania the Inspection Entity is the Ombudsman.
5. Additionally, every record or report obtained through the use of a surveillance device is to be kept in a secure place by the Chief Officer of the law enforcement agency who must ensure that any such record or report is destroyed if it is not likely to be required for one of the purposes under s. 34 of the Act.

At an early stage of the Review I researched the reports of inspections undertaken by the Ombudsman's Office, as the Ombudsman is the Inspection Entity appointed by the Minister under s. 40 of the Act, to determine the level of compliance reported by the Ombudsman.

The reports of inspections in the Ombudsman's Annual Reports did not seem to me to comply with the requirements of the Act for Inspection Entity inspections and reporting.

THE OMBUDSMAN AND THE ROLE OF INSPECTION ENTITY.

Section 41(1) of the Act provides that:-

“The inspection entity must, from time to time and at least once every twelve months, 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.”

Authority to enter the agency and undertake inspections is provided for in the balance of section 41 and s. 42, dealing with the Report on Inspection, provides in subsection (1) :-

“(1) The inspection entity must make a written report to the Minister and the Minister administering the Police Service Act 2003 by not later than 3 months after the end of each financial year on the results of each inspection under s. 41.” And in subsection (2) of s. 42 :-

“(2) The report referred to in subsection (1) is to include a report on the comprehensiveness and adequacy of the records of the agency and the cooperation given by the agency in facilitating the inspection of those records.”

I attach marked ‘D1’ a copy of a section of the Ombudsman’s Annual Report for 2022/2023, page 38, where details the report of the inspection under the Act for that year appear. I have also attached, marked ‘D2’, a copy of the report tabled in Parliament for the inspection undertaken in June 2021. These reports are brief and suggest compliance with s.42(2) but not s.42(1).

I met with the Ombudsman on two occasions. Before we met in December 2023, the Ombudsman’s Office provided me with details of legal advice in 2009 which the then Ombudsman received from a senior lawyer from another Government legal office who was on secondment to the Ombudsman’s Office at that time. Based on that advice, provided when the Act commenced, the Ombudsman’s office has conducted annual inspections of the records kept by Tasmania Police and reported accordingly.

Our discussion in December centred on the inspections and reporting undertaken by the Ombudsman’s office and whether they were compliant with the provisions of the Act. After that meeting, during January, I was able to clarify the statutory requirements for inspections and reporting. I met with the Ombudsman again in February.

I am satisfied that the reporting by the Inspection Entity, the Ombudsman, complies with s. 42(2), “the comprehensiveness and adequacy of the records of the agency and the cooperation given by the agency”, but there has been no reporting on compliance, under s. 41, since the Act commenced in 2009.

The Ombudsman, Mr Connock, has been amenable to finding a resolution of the question and trying to determine the best way forward. He is in the uncomfortable position of inheriting a process instituted 14 years ago on legal advice which was either wrong or incomplete. In my view the advice was wrong.

The reality is that for 14 years reports have been prepared which are only an audit of the comprehensiveness and adequacy of the records kept by the agency. There has been no evaluation of the Department's, and its officers,' "compliance with the Act" as required by s. 41 in that time.

I am confident, from the discussions I have had with Mr. Connock, and the Deputy Ombudsman, Ms Clare Hopkins, that the Office does not have the resources to undertake the inspection and reporting as required by the Act. In the long term something must be done for the budget of the Ombudsman's office as I have had another recent experience of the pressures of workload on that Office.

I discussed with you, in mid-December, a possible solution for the problem which this discovery had unearthed. The records which must be inspected, especially for the evaluation of compliance more generally, are classed as "protected information' under the Act and there are access prohibitions, with few exceptions. There is an argument that the amendment to the Act in September 2023 which gave me an exemption, under s. 33, to inspect protected information for this Review will permit an amendment to the Terms of Reference to extend the Review. But I am not confident that the words "as amended from time to time" in s. 33 (3A)(a), have the meaning which would permit such a broadening of the Review Terms. This is a Review in to the use of surveillance devices "in prison," not more generally. Anyway, I did not have the time or the resources to contemplate such a task and, as discussed at the time, that will only extend an already delayed completion of this Review, and probably require another amendment of the Act to be taken to Parliament. We discussed the matter again in January.

The period of 14 years of incomplete inspections, more importantly inspections and reporting to the Minister and Parliament on compliance with the Act, is a matter of concern which should be addressed. I am surprised it has not been noticed before now.

It was not appropriate that in my Report to you I should highlight an issue and leave questions hanging only to see another review initiated. We discussed a possible solution, which would incorporate one of the recommendations I was contemplating after my interviews with the 16 applicant officers.

INSPECTION OF 14 YEARS OF RECORDS.

Under s. 33 the prohibitions on communication or publication of protected information do not apply to 'training of police officers'.(s.33(4)(ga)). This exemption provides a possible, and acceptable solution.

An internal review of the old records, and an independently overseen inspection to determine statutory compliance, while using an analysis of the learnings from the outcome to assist in developing the training module being established at the Academy would, I thought, overcome the immediate concerns for the 14 years of missed inspections with the added advantage of the development of a very useful module or training tool using the existing exemption under the Act.

You have taken independent advice from a respected senior auditor in Hobart who, understanding the backlog and the role of a compliance inspector, has advised that 10% of matters is an acceptable selection of matters to undertake a credible compliance inspection.

The Commonwealth Ombudsman uses an 11% sample of files when that Office undertakes similar inspections under the equivalent Commonwealth legislation. I am attaching, marked 'E,' an extract from the 2008 annual report of the Commonwealth Ombudsman on the inspection by that office of the records of the Australian Federal Police for that year. These records and the report are similar to those which should be inspected and reported on by the Ombudsman in Tasmania. It is interesting, as an aside, to note the focus on privacy issues in the processing of warrant applications. The same issue was the subject of comment by the Ombudsman in an earlier report on its review of NSW Police records. (Hence my comment earlier that privacy concerns were not just a Tasmanian issue).

You have tasked Ms Rebecca Munnings LLB (Hons), Senior Legal Officer from your Legal Services Division to undertake a 10% sampling and inspection of records over the 14 years during which no s.41 compliance reporting has occurred. While the task is aimed at providing a practical understanding from the records to inform a training module for use at the Academy, the exercise has also provided a useful compliance inspection, with audit approval, spanning the last 14 years of records of surveillance warrant activity in Tasmania. I have examined the results and the inspection and compliance reporting has been more detailed than I would expect of a compliance inspection under the Act. That is understandable because of the 'training' module target of the exercise. The compliance element of Ms. Munnings' work has detected 'fine tuning' issues in some matters. They are not of any structural or deep seated concern. I have not seen any of the records inspected, but the detail of the depth of inspection undertaken covers more than just statutory compliance.

The implementation of those 'learnings' in to a training exercise will, I am sure, more than satisfy what I would have recommended as a refresh training module.

In terms of a compliance inspection, I would not add anything further, I regard the outcome as an appropriate inspection and review of what are now old records, and something which should provide reassurance. I consider that what I have done in independently overseeing the completed report is covered by TOR 5.

The calling of the election earlier this year provided time for this exercise to be undertaken and I have held back reporting to you so that I could include mention of what has happened in my Report which must be tabled in due course.

ARE OTHER SAFEGUARDS NEEDED?

I suspect that the issues I have examined and the lack of compliance inspections and reports for 14 years will provoke a demand for additional oversight, suggesting that the system requires fixing. I would caution against a knee jerk response. How does another safeguard fit with what is there? We do not need another oversight body, we have one at present. It will now conduct inspections on a correct application of the law, but it is seriously under resourced. Interestingly, the reports, tabled in Parliament for 14 years, were not detected as non- compliant with s. 41(1)

Other states, Victoria and Queensland have an independent office holder, the Public Interest Monitor (PIM.) The role of the PIM in those states (Queensland has had one for 25 years and I know the current office holder.) involves appearances at hearings of applications for surveillance device warrants and raising questions if there are concerns that matters such as privacy are not adequately addressed on the papers. The PIM represents the public interest in the hearing, Each application is critically examined on the papers first and if there are questions to be raised or submissions to be made the PIM will attend the hearing if those matters cannot be resolved beforehand.

In Queensland the PIM, Mr David Adsett, routinely looks for things such as :-

Is the offence one for which a warrant is issued?

Are the statutory criteria for an application otherwise met?

Is the offence correctly stated?

Are the issuing criteria addressed?

What is likely to be said which is relevant to the nominated offence?

Are the conditions appropriate? (consideration of LPP and other people's privacy)

Are the application and draft warrant consistent?

Are the conditions in the warrant consistent with the what the application sought?

COMMENT.

1. ANOTHER OVERSIGHT/SAFEGUARD ENTITY.

I would expect that the scrutiny now applied internally to the application process will insist that a similar pre hearing checklist be applied. This will ensure that issues such as those considered by the Queensland PIM, and interestingly very similar to part of the checklist I created for my own use, are either dealt with or anticipated. They will certainly be available in the documents open for a full inspection to the Inspection Entity. This is why I placed emphasis on the Section 29 report in the Recommendation section.

I think that it would be premature to rush to something like an office of PIM at this stage. I had the opportunity to discuss the work of the office with the Queensland PIM when he was in Tasmania earlier this year and I am happy to expand on my reasons for taking this position should it become necessary.

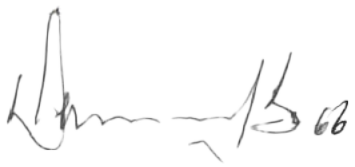
There are internal changes which have been and are being made and recommendations in this Report. I suggest that a system, which in my view is not broken but needs fine tuning, should be given an opportunity to work with those changes and enhanced oversight, hopefully with an improved budget for the Office of the Ombudsman, for which I will make independent submissions. If there are insufficient resources for the Office with the inspection function under the Act, it is difficult to see an immediate response to any suggestion for an additional 'inspection' functionary in any event.

2. BREADTH OF TERMS OF REFERENCE

I have commented on the breadth of the terms of reference and it is a matter which has been raised with me by people I have spoken to. The question of the limitation of the Review Terms of Reference to the warrants issued in relation to prison surveillance and the scope of the Review was raised as a possible limitation. It was suggested that the Review should be widened to cover other warrants, "is there an issue which has been highlighted by the decisions in the Thompson case which should be examined across all warrants," and should there be another layer of oversight within the Act, a PIM, which extends the safeguards already there?

The changes implemented following the internal review, the recent internal but extended scrutiny of 14 years of unchecked records, independently overseen, bringing new learnings to training, together with the matters this Review has considered and recommended, should be allowed to run their course. I did not detect any attempt to avoid scrutiny. The records held by the Department, while protected information under the Act, were available for my inspection and have been inspected annually by the Ombudsman's Office, albeit under s. 42. In addition I received full cooperation from the more than 30 police officers I interviewed, every record I asked for was provided, all arranged by the able assistance I received from Senior Legal Officer Rebecca Munnings of the Legal Services Division.

I conclude by expressing my appreciation for the support which you and Assistant Commissioner Blackwood and Senior Officers of the Department provided throughout this Review.



A

Review of the use of Surveillance Devices in Prisons

TERMS OF REFERENCE

TRIM: A23/220654

Updated: v3 14 September 2023

Tasmanian Government

1. Background/Context

In June 2017, a police officer involved in an investigation into an alleged conspiracy to pervert the course involving Jeffrey Ian Thompson and five other persons applied to a magistrate for the issue of a surveillance device warrant under the *Police Powers (Surveillance Devices) Act 2006*. The warrant was sought to authorise the recording of meetings between a prisoner, Stephen Gleeson, and Mr Thompson or other persons suspected of engaging in the conspiracy.

The application for a surveillance device warrant was made in response to information obtained by Tasmania Police that Mr Thompson and others were attempting to have Mr Gleeson produce false evidence for use in Ms Sue Neill-Fraser's application for leave to appeal and subsequent second appeal against her conviction for the 2009 murder of Bob Chappell.

A magistrate issued a surveillance device warrant on 12 June 2017 for a period of 90 days. The warrant authorised the installation and use of surveillance devices in visitor rooms at the Risdon Prison complex utilised by Mr Gleeson. On 15 June 2017, police installed two devices in a meeting room at the Prison. They were retrieved on 17 August 2017. One device recorded conversations to a hard drive. Police could directly monitor the other device. The only occasion it was monitored was on 16 June 2017 whilst a meeting between Mr Thompson and Mr Gleeson took place. The hard drive which recorded conversations was accessed by police on 21 June 2017. The only conversation listened to by police was the conversation between Mr Gleeson and Mr Thompson on 16 June 2017. That was the only conversation retained by police. Whilst the surveillance devices remained in place until 17 August 2017, no further use was made of their product after 16 June 2017.

The conversation which occurred between Mr Thompson and Mr Gleeson on 16 June was not subject to legal professional privilege because Mr Thompson was not acting in his professional capacity as a lawyer at the time or assisting a lawyer. In any event, legal professional privilege does not protect communications made in furtherance of the commission of a criminal offence.

Whilst the hard drive may have captured private conversations unrelated to the investigation, and potentially conversations which were subject to legal professional privilege, they were not listened to, or retained by, Tasmania Police.

The conversation between Mr Thompson and Mr Gleeson on 16 June 2017 led to both of them being indicted by the Director of Public Prosecutions for the crime of pervert justice. Mr Gleeson pleaded guilty to that crime in March 2018 and was sentenced to 12 months imprisonment.

Mr Thompson pleaded not guilty to two counts of pervert justice. His trial commenced before Justice Brett in March 2022. His Honour ruled the surveillance device warrant to be unlawful as it referred to Section 297(2) of the *Criminal Code*, rather than Section 297(1), which creates the offence of conspiracy to pervert justice. As a result of that ruling, His Honour was required to exercise a discretion whether to permit the evidence obtained under the warrant to be admitted into evidence on the trial of Mr Thompson. His Honour excluded the evidence based on his concern that the application for the surveillance device warrant did not adequately address the risk of surveillance devices installed in the meeting room at the Risdon Prison complex capturing private conversations unrelated to the investigation, including conversations which were subject to legal professional privilege.

In his judgement concerning the exercise of his discretion, handed down on 28 July 2022, Justice Brett expressed his satisfaction "that the police made a genuine attempt to obtain the relevant lawful authorisation and, believed, and were entitled to believe, that the warrant had been validly issued before they recorded the conversation."

His Honour also acknowledged that "while it appears that police did not deliberately set out to break the law, there was also an obvious misunderstanding or ignorance of the significant risks inherent in their task."

Tasmania Police took immediate steps to address the issues identified in Justice Brett's decision. An initial internal review of procedures to ensure there is clear guidance to police officers in relation to the obtaining of surveillance device warrants and the execution of warrants has been completed, with new procedures implemented. The Commissioner has also committed to an independent review of the use of surveillance devices in prisons.

2. Definitions

Prison	includes a place of detention irrespective of the title by which it is known, and includes the whole area, whether or not walled or fenced, established as a prison (*Corrections Act 1997*).
legal professional privilege	is a common law right that exists to protect the administration of justice and the right of an individual to obtain confidential advice about their legal circumstances. It protects legal advice given by a lawyer to his or her client and communications pertaining to actual or contemplated litigation or court proceedings.

3. Objective

The independent review will involve consideration of all surveillance device warrants issued to Tasmania Police officers since 1 January 2012 which authorised the installation and use of a surveillance device in a prison. It will consider the adequacy of information included in the applications for those warrants and compliance with any conditions or limitations imposed on the warrants. The reviewer will be requested to identify any improvements which could be made in applications for the issue of surveillance device warrants or the execution of such warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought and to prevent access to, or retention of, any such conversations.

4. Scope

The review will:

1. Review all surveillance device warrants issued to Tasmania Police officers since 1 January 2012 to the present day which authorised the installation and use of a surveillance device in a prison.

2. Consider the adequacy of the information provided to issuing officers in applications for the use of surveillance device warrants within the scope of the Review in relation to:

    i. the risk of the use of the surveillance resulting in the capture of private conversations unrelated to the investigation in respect of which the warrant was sought;

    ii. proposed measures to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.

3. Consider the adequacy of any conditions or limitations imposed by issuing officers on surveillance device warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.

4. Consider compliance by Tasmania Police with any conditions or limitations referred to in paragraph 3 and the adequacy of any measures taken by Tasmania Police of its own volition to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which the warrant was sought and to prevent access to, or retention of, any such conversations.

5. Identify any improvements which could be made in applications for the issue of surveillance device warrants or the execution of such warrants to mitigate the risk of capturing private conversations unrelated to the investigation in respect of

which a warrant is sought and to prevent access to, or retention of, any such conversations.

6. Consider whether any specific measures are required to mitigate the risk of capturing private conversations unrelated to the investigation in respect of which a warrant is sought which may be subject to legal professional privilege and to prevent access to, or retention of, any such conversations.

5. Approach

The review will be undertaken independently of Tasmania Police.

Tasmania Police is fully supportive of this review and will assist the reviewer with any requests to access staff and records.

6. Deliverables

At the conclusion of the review, a report will be prepared outlining the reviewer's findings and recommendations.

This report will be tabled in Parliament.

Pre-execution: Copy to be forwarded to Surveillance Services Coordinator & SCS as soon as possible.
Post-execution: Original to be provided to Surveillance Services Coordinator & SCS on request.

Tasmania Police SDW NUMBER
(SCS use only)

APPLICATION FOR SURVEILLANCE DEVICE WARRANT

COURT DETAILS

Magistrate/Supreme Court of Tasmania (Delete whichever does not apply)

Insert Court Address

MATTER

Application under section 9 of the *Police Powers (Surveillance Devices) Act 2006* for a surveillance device warrant.

APPLICANT'S DETAILS

Filed By Insert name of applicant

Address Station
Address
Telephone: (03)

APPLICATION

1. I insert name of applicant am a insert rank in the Tasmania Police Service and am a law enforcement officer for the purposes of the *Police Powers (Surveillance Devices) Act 2006 ('the Act')*

2. I make application for the issue of a surveillance device warrant under section 9 of the Act

3. A surveillance device warrant is sought to authorise:

the use of a:

- ☐ Data surveillance device(s)
- ☐ Listening device(s)
- ☐ Optical surveillance device(s)
- ☐ Tracking device(s)

on or in premises, namely: insert details of the premises

and/or:

Pre-execution: Copy to be forwarded to Surveillance Services Coordinator & SCS as soon as possible.
Post-execution: Original to be provided to Surveillance Services Coordinator & SCS on request.

the use of a:

- ☐ Data surveillance device(s)
- ☐ Listening device(s)
- ☐ Optical surveillance device(s)
- ☐ Tracking device(s)

in or on an object or class of objects, being: insert object details

and/or:

the use of a:

- ☐ Data surveillance device(s)
- ☐ Listening device(s)
- ☐ Optical surveillance device(s)
- ☐ Tracking device(s)

in respect of the conversations, activities or geographical location of:

- a specified person, namely [insert name of person]; or
- a person whose identity is unknown. (Omit whichever does not apply)

4. A surveillance device warrant is sought for a period of insert number of days.

5. This Application is accompanied by my Affidavit sworn on insert date.

Signed:

Full Name Insert name of applicant

Date: Insert date

Original to be forwarded to Surveillance Coordinator $ SCS as soon as it has been signed.

Tasmania Police SDW Number
(SCS Use Only)

SURVEILLANCE DEVICE WARRANT

Police Powers (Surveillance Devices) Act 2006

I, ...,
a Judge of the Supreme Court*/Magistrate*,
hereby issue a surveillance device warrant under section 11 of the *Police Powers (Surveillance Devices) Act 2006* ('the Act').

1. The applicant for the warrant is: insert name of applicant.
2. The law enforcement officer primarily responsible for executing the warrant is: insert the name of the officer primarily responsible for executing the warrant.
3. The alleged offence in respect of which the warrant is issued is: insert the relevant offence under investigation.
4. I am satisfied of the matters referred to in section 11(1) of the Act, namely:
   a) that there are reasonable grounds for the suspicion or belief founding the application for the warrant; and
   b) in the case of an unsworn application, that it would have been impracticable for an affidavit to have been prepared or sworn before the application was made; and
   c) in the case of a remote application, that it would have been impracticable for the application to have been made in person.
5. In issuing this warrant, I have had regard to:
   a) the nature and seriousness of the alleged offence in respect of which the warrant is sought; and
   b) the extent to which the privacy of any person is likely to be affected; and
   c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation; and
   d) the evidentiary or intelligence value of any information sought to be obtained; and
   e) any previous warrant sought or issued under Part 2, Division 2 of the Act, a corresponding law or the *Listening Devices Act 1991* in connection with the same offence.

6. In the case of a warrant for the use of a surveillance device on premises: (*strike out if not applicable)
    a) The warrant authorises the use of the following surveillance devices(s)
        ☐ data surveillance device
        ☐ listening device
        ☐ optical surveillance device
        ☐ tracking device
    b) The warrant authorises the use of the surveillance device on the following premises: insert details of the premises.
    c) The warrant authorises entry to the following premises in relation to the use of the surveillance device: insert details of any other premises which may be entered.
    d) The premises may be entered subject to the following conditions:
        .....
        .....
        .....
        .....
        .....
        .....
        .

7. In the case of a warrant for the use of a surveillance device in or on an object or class of objects*: (strike out if not applicable)
    a) The warrant authorises the use of the following surveillance devices(s):
        ☐ data surveillance device
        ☐ listening device
        ☐ optical surveillance device
        ☐ tracking device
    b) The warrant authorises the use of the surveillance device in or on the following object or class of objects: insert details of the object/class of objects.
8. In the case of a warrant for the use of a surveillance device in respect of the conversations, activities or geographical location of a person*. (*strike out if not applicable)
    a) The warrant authorises the use of the following surveillance devices(s):
        ☐ data surveillance device
        ☐ listening device
        ☐ optical surveillance device
        ☐ tracking device
    b) The warrant authorises the use of the surveillance device in respect of the conversations, activities or geographical location of:
        (i) the following person: insert details of the person*, or
        (ii) a person whose identity is unknown* (*strike out which ever does not apply)

9. In the case of a warrant which authorises the use of a surveillance device in a participating jurisdiction:
    a) The warrant authorises the use of a surveillance device in the following participating jurisdiction: insert the name(s) of the participating jurisdictions(s).
10. The warrant authorises the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the installation, use, maintenance or retrieval of a surveillance device or enhancement equipment under the warrant.
11. The surveillance device may be used subject to the following conditions:
    .....
    .....
    .....
    .....
    .....
    .....
    .....
12. Premises may be entered subject to the following conditions:
    .....
    .....
    .....
    .....
    .....
    .....
13. The warrant is issued on:
14. The warrant is issued at: am / pm
15. The warrant is in force for a period of 90 days.
16. The applicant or the law enforcement officer who is primarily responsible for executing the warrant is to make the report required by section 29 of the Act within 60 days (*vary if required*) from the expiration of the warrant (including any extension thereof).

Signature .....

Full name .....

Supreme Court Judge / Magistrate

Checked and Authorised .....
(Inspector)
Date .....

C

To be forwarded via the Surveillance Services Coordinator, Serious Crime Support

Tasmania Police SDW NUMBER
(SCS use only)

REPORT UNDER SECTION 29
POLICE POWERS (SURVEILLANCE DEVICES) ACT 2006

SURVEILLANCE DEVICE WARRANT

COURT DETAILS

Magistrate/Supreme Court of Tasmania (Delete whichever does not apply)

Insert Court Address

MATTER

I submit this report in accordance with section 29 of the *Police Powers (Surveillance Devices) Act 2006.*

A. WARRANT DETAILS

Warrant Reference Number	Insert number
Date of Issue	Insert date when the warrant was issued
Person who issued the warrant	Insert name and Court
Person to whom the warrant was issued	Insert name

B. EXECUTION OF WARRANT – Section 29(3)(a)

The warrant was/was not executed. ***If the warrant was not executed, delete section C.**

C. EXECUTION DETAILS – Section 29(3)(b)

Date & time on which the warrant was executed	Insert date & time

The name of the person primarily responsible for the execution of the warrant	Insert name of the person
Name of each person involved in the <u>installation</u> of the surveillance device	Insert name of every person
Name of each person involved in the <u>maintenance</u> of the surveillance device	Insert name of every person
Name of each person involved in the <u>retrieval</u> of the surveillance device	Insert name of every person
Type of surveillance device used	Insert details of the device
Period during which the device was used	From start date to end date.

The name (if known) of any person whose conversations or activities were <u>overheard</u>	Insert names if known
The name (if known) of any person whose conversations or activities were <u>recorded</u>	Insert names if known
The name (if known) of any person whose conversations or activities were <u>monitored</u>	Insert names if known
The name (if known) of any person whose conversations or activities were <u>listened to</u>	Insert names if known

The name (if known) of any person whose conversations or activities were observed	Insert names if known
The name (if known) of any person whose geographical location was determined by the use of a tracking device	Insert names if known
The premises on which the device was installed	Insert details of the premises
The place at which the device was installed	Insert details of the place
The object in or on which the device was installed	Insert details of the object

The premises where the object was located when the device was installed	Insert details of the premises
The benefit to the investigation of the use of the device	Insert details of what benefit the use of the device had for the investigation
The general use made or to be made of any evidence or information obtained by the use of the device ** SURVEILLANCE DEVICE INFORMATION OBTAINED HAS BEEN/WILL BE GIVEN IN EVIDENCE – GIVE DETAILS**	
Compliance with the conditions to which the warrant was subject (if any)	Provide a statement as to whether the conditions stated in the warrant were complied with
Number of extensions to the warrant (if any)	State number, if there were any
Reasons for the extensions	State reasons, if an extension was sought
Number of variations to the warrant (if any)	state number, if there were any

Reasons for the variations	State reasons, if an extension was sought

Signed:

Rank and Name
Officer to whom the warrant was granted or
Officer primarily responsible for executing the warrant

Date:

Forwarded by Surveillance Services Coordinator
Serious Crime Support

Date:

Tasmania Police SDW NUMBER
(SCS use only)

POLICE POWERS (SURVEILLANCE DEVICES) ACT WARRANT RETURN – SECTION 29

RE INSERT NAME

Received by Chief Magistrate or Supreme Court on day of 20

Received by:

Received From:

Please return this transmission receipt to:

Surveillance Services Coordinator
Serious Crime Support
Tasmania Police
P.O. Box 308C
GPO HOBART 7001

The Ombudsman is the inspection entity in relation to certain records that must be retained by law enforcement agencies.

Police Powers (Surveillance Devices) Act 2006

This Act provides for the installation, use, maintenance and retrieval of surveillance devices in criminal investigations and other matters. It is the role of the inspection entity to ensure that law enforcement agencies in Tasmania (principally Tasmania Police and the Integrity Commission) comply with their record-keeping obligations under the Act. My delegated officers conduct inspections of records held under the Act at least once every year and I make a written report to the relevant ministers on the results of each inspection. The Minister for Justice then causes a copy of the report to be laid before each House of Parliament. A copy of my latest report on this financial year's inspection can be obtained through Hansard on the Parliamentary website.

Police Powers (Controlled Operations) Act 2006

This Act provides for the authorisation, conduct and monitoring of controlled police operations. As with the Surveillance Devices Act, it is the role of the inspection entity to ensure that law enforcement agencies comply with their record-keeping obligations under the Act and, again, a copy of my latest report on the inspection can be obtained through Hansard.

Telecommunications (Interception) Tasmania Act 1999

Tasmania Police is obliged to keep certain specified records relating to telecommunications interceptions. These records must be inspected by my office at least once every six months to ensure Tasmania Police is complying with its obligations. I am required to report to the relevant minister on the inspections at the end of each financial year. The minister must then provide a copy of the report to the relevant Commonwealth minister. My officers conducted inspections in December 2022 and June 2023. As in preceding years, Tasmania Police was at all times cooperative in facilitating inspections and I was satisfied with the comprehensiveness and adequacy of the records maintained.

Misuse of Drugs Act 2001

Section 38B of the *Misuse of Drugs Act 2001* allows the Commissioner of Police to issue authorisations for police officers, employees or correctional officers (authorised persons) to possess and supply controlled substances, such as heroin, cocaine, cannabis and methylamphetamine hydrochloride. The purpose of the Commissioner of Police issuing an authorisation under section 38B to authorised persons, is to allow for the possession and supply of controlled substances to be used for the training and assessing of drug detection dogs and the transport of the controlled substances to other police officers, interstate or federal police officers or correctional officers. I am required under section 38I of the Act to prepare a report, after receiving an operational report from the Commissioner of Police, setting out:

(a) a summary of the matters provided in the operational report;

(b) my opinion as to the comprehensiveness and adequacy of the records of the Commissioner of Police kept under section 38G;

(c) my opinion as to whether the authorisations to which the operational report relates have been effective and appropriate; and

Ombudsman Tasmania

Level 6, 86 Collins Street, Hobart
GPO Box 960, Hobart Tas 7001
Phone: 1800 001 170
Email: ombudsman@ombudsman.tas.gov.au
Web: www.ombudsman.tas.gov.au

11 August 2021

Report on inspections under the *Police Powers (Surveillance Devices) Act 2006* and the *Police Powers (Controlled Operations) Act 2006*

The Ombudsman has been appointed as an inspection entity under the *Police Powers (Surveillance Devices) Act 2006* (the Surveillance Devices Act) and the *Police Powers (Controlled Operations) Act 2006* (the Controlled Operations Act).

Surveillance Devices Act

The Surveillance Devices Act came into effect on 1 January 2009. It governs the use that a law enforcement agency makes of surveillance devices and also the records that it is obliged to keep in respect of each warrant for which it applies. The Ombudsman is required to inspect the records of a law enforcement agency from time to time, but at least once every 12 months. Under section 41 of the Act, the inspection is conducted in order to determine the extent of the compliance with the Act by the agency as well as the law enforcement officers of the agency. I am obliged under section 42 to make a written report which includes a report on the comprehensiveness and adequacy of the records of the agency and the cooperation given by the agency in facilitating the inspection.

My delegated officers inspected Tasmania Police's records on 23 June 2021. I am satisfied with the comprehensiveness of Tasmania Police's records. Tasmania Police offered assistance during the inspection and the relevant staff were cooperative at all times in facilitating the inspection of the records.

Controlled Operations Act

The Controlled Operations Act came into effect on 1 September 2009. It provides for the authorisation, conduct and monitoring of the controlled operations. A controlled operation means an operation that is conducted for the purpose of obtaining evidence that may lead to a prosecution. Such operations often involve controlled conduct, that is conduct a person would be criminally responsible for but for the exemptions in the Controlled Operations Act.

The Controlled Operations Act contains very similar provisions to the Surveillance Devices Act with respect to the role of the inspection entity. My officers inspected Tasmania Police records held in accordance with this Act on 23 June 2021. In terms of Tasmania Police's compliance with the record keeping requirements of the Controlled Operations Act, there were no changes of any significance since the last inspection and I am satisfied with the comprehensiveness and adequacy of the agency's controlled operations records. The relevant Tasmania Police officer was cooperative at all times in facilitating the inspection.

Richard Connock
OMBUDSMAN

Part 4: AUSTRALIAN FEDERAL POLICE

Inspection details – Surveillance device records

4.1. From 6 to 10 March 2023, we inspected the AFP's surveillance device records. We inspected records of warrants and authorisations that expired between 1 January and 30 June 2022.

4.2. The available records consisted of 7 refused warrants, 346 surveillance device warrants (including 12 control order and supervisory order surveillance device warrants), 11 retrieval warrants, 5 tracking device authorisations, 74 destructions and 44 retentions of protected information.

Table 5: Summary of records for AFP surveillance devices inspection

	Records made available	Records inspected
TOTAL	**487**	**55 (11%)**

Progress since our previous inspection

4.3. We last publicly reported inspection results for the AFP in our September 2022 report to the Minister. That report included findings in relation to non-compliance with destruction requirements of the Act and instances of section 49 reports not being made to the Minister in accordance with the Act.

4.4. At this inspection we confirmed that the AFP took appropriate remedial action in relation to the previous findings.

Inspection findings

Finding – Insufficient information concerning privacy considerations in applications for surveillance device warrants

4.5. We identified that several applications for surveillance device warrants (including supporting affidavits) did not sufficiently outline the extent to which the privacy of any person would likely be affected by the warrant, for consideration by the eligible judge or nominated Administrative Appeals Tribunal (AAT) member under section 16(2)(c) of the Act. We found that standard template

wording was used for applications involving more than one target and did not outline the potential privacy implications based on the individual circumstances of the case.

4.6. While we recognise that the issuing authority must have regard to privacy, we consider it prudent that the affidavit addresses the extent to which the privacy of any person is likely to be affected to demonstrate that sufficient information was provided to the issuing authority.

4.7. We suggested, as a matter of better practice, the AFP ensure there is sufficient information in applications addressing the privacy considerations of any person likely to be affected by the warrant.

4.8. The AFP accepted our suggestion and committed to reviewing relevant warrant application templates to ensure guidance on addressing privacy considerations is comprehensive and consistent. The AFP also stated that it will provide guidance to applicants and those responsible for quality assurance on when to include additional information to demonstrate the privacy impact has been considered reasonably and proportionately.

Inspection details – Digital surveillance records

4.9. From 6 to 10 March 2023, we inspected the AFP's digital surveillance records. We inspected records of computer access warrants that expired between 1 January and 30 June 2022, and data disruption warrants that expired between 3 September 2021 and 30 June 2022.

4.10. The available records consisted of 6 computer access warrants, 1 data disruption warrant, 2 computer access warrant destructions and 1 computer access warrant retention.

Table 6: Summary of records for AFP digital surveillance inspection

	Records made available	Records inspected
TOTAL	**10**	**10 (100%)**

Inspection findings

4.11. We made no findings and were satisfied that the AFP was compliant when using computer access warrants and data disruption warrants.