Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee

on its inquiry into

the provisions of the Surveillance Devices Bill 2004

23 April 2004

Table of Contents

The Privacy Commissioner acknowledges the work of Michelle Fisher, Senior Policy Officer, in the preparation of this document.

SENATE LEGAL AND CONSTITUTIONAL COMMITTEE INQUIRY INTO THE PROVISIONS OF THE TELECOMMUNICATION (INTERCEPTION) AMENDMENT BILL 2004

Summary of Privacy Commissioner's recommendations

1 Further consideration should be given to enhancing safeguards and public oversight by, eg, requiring notification to persons under surveillance, in circumstances in which that would be appropriate. Consideration should also be given to adopting legislation that is technology-neutral.

2 Clause 14(5) of the Bill should be amended require an application for a surveillance devices warrant to specify any object or system that may be used [under clause 18(3)(f)] to transmit information in connection with the operation of a surveillance device.

3 Optical and tracking surveillance devices should only be used with appropriate judicial oversight.

4 Surreptitious recording of conversations by or on behalf of police should only occur with appropriate judicial oversight.

5 Law enforcement agencies should be required to report back to the judge, so that the judge can consider whether the surveillance device warrant should be revoked or other action taken.

6 The general conduct of any surveillance by police should be subject to independent oversight by the Ombudsman and the extent and effectiveness of its use be made known to the public through Parliament. If Parliament nevertheless decides to permit warrantless surveillance, then the reporting requirements in Part 6, Division 2 should include a requirement to report on the use, extent and effectiveness of warrantless surveillance.

7 Clause 46 should be amended to require independent oversight (eg, by the Ombudsman) of any decision by police to destroy surveillance records, prior to their destruction.

I. Introduction & Background

1 As noted by the Commonwealth Attorney-General, the Hon. Philip Ruddock, in his Second Reading Speech on 24 March 2004:

> [The Surveillance Devices Bill 2004 (Cth)] began as an initiative of the leaders summit on terrorism and mutijurisdictional crime held on 5 April 2002.
>
> A joint working group of Commonwealth, state and territory officials was established by the Standing Committee of Attorneys-General and the Australasian Police Ministers Council.
>
> The joint working group ["JWG"] developed comprehensive model laws for all Australian jurisdictions to improve the effectiveness of cross-border criminal investigations in the areas of controlled operations, assumed identities, protection of witness identity and electronic surveillance,
>
> These model laws were released in a public discussion paper to solicit feedback from groups and individuals on the suitability of the proposed powers.
>
> This bill implements the electronic surveillance model bill, tailoring it to the needs of the Commonwealth.

2 This Office made a submission to the JWG during its consultation on the above-mentioned model laws. The consultation period ran for two weeks, from 7 March 2003 to 28 March 2003. An extension of time was granted until the end of April 2003, when this Office made an initial submission. The final (slightly revised) version, dated 5 June 2003, is attached.

3 This Office's submission focussed on the model surveillance devices bill. The Committee will note that a number of issues were discussed in some detail in my submission, and many others simply noted (in Part V) due to the limited time available for comment.

4 Some of the significant matters that remain unresolved in the final draft of the Surveillances Devices Model Bill ("Model Bill") include:

a. the desirability of a Public Interest Monitor, similar to that which exists in Queensland, to be incorporated in the Bill;

b. notification to subjects of surveillance, where appropriate;

c. ensuring that the surveillance is not authorised where it would be contrary to the local privacy law if it were engaged in by a law enforcement agency subject to that law;[1]

d. regulating surveillance in public places;

e. regulating participant monitoring by and on behalf of police;

f. requiring substantial similarity of surveillance laws as a pre-condition to mutual recognition;

g. developing technology-neutral legislation to better encompass existing and emerging surveillance devices;

h. regulating converging technology that currently cross, or fall short of, existing regulatory schemes (eg, convergence of telecommunications, stored communications and broadcasting capability in mobile telephones).

Recommendation: Further consideration should be given to enhancing safeguards and public oversight by, eg, requiring notification to persons under surveillance, in circumstances in which that would be appropriate. Consideration should also be given to adopting legislation that is technology-neutral.

5 For brevity's sake, the comments that follow focus on those areas where the Commonwealth Bill has departed from the Model Bill.

6 The Committee's attention is drawn to the Introduction section of my Submission:

> 4 The need for operational efficiency in carrying out cross-border investigations into unlawful criminal activity is acknowledged. Criminals do not necessarily confine their activity to a single jurisdiction. Crimes are increasingly committed across state borders with the use of existing and emerging technologies. Members of the public legitimately expect law enforcement agencies to be equipped with the necessary tools and powers to investigate unlawful activity so as to protect the community from harm and ensure alleged offenders can be prosecuted….
>
> 10 Privacy is not necessarily antithetical to the interests of law enforcement. In many ways, privacy principles can enhance the legitimacy and integrity of surveillance activities engaged in by police by, for instance:
>
> a. limiting collection of personal details to what is necessary to achieve the police force's legitimate aims of prevention, detection and investigation of crime;
>
> b. requiring the use of personal information to be in accordance with these aims;
>
> c. demanding secure storage of personal information after it has been collected; and
>
> d. requiring its destruction or de-identification when the information is no longer needed.
>
> 8 Where privacy is to systematically give way to other public interests, it should only do so:
>
> a. under the authority of law;
>
> b. to the extent necessary to achieve precise objectives that have been articulated in advance by the relevant decision makers; and
>
> c. with safeguards and accountability measures built into any authorising legislation to ensure the use of such intrusive powers is restrained and not abused.
>
> 9 The spectre of unrestrained surveillance by law enforcement agencies is to be resisted if we are to maintain a society where individuals' civil liberties, of which privacy is a slice, are to be respected. History informs us that the potential for misuse of surveillance powers is not mere speculation. Examples include:
>
> a. in February 2003, the *Herald Sun* reported that a confidential report prepared by the Victorian Ombudsman in December 2001 (but not publicly released) criticised Victoria Police for the accuracy and completeness of some of its affidavits used in support of applications for listening device warrants;[2]
>
> b. in October 1997, *The Age* published a series of articles concerning the activities in the late 1980s and early 1990s of Victoria Police relating to the surveillance and monitoring of individuals and groups in the community. The Victorian Ombudsman conclude that a great deal of information had been gathered about people who, in the vast majority of instances, were targeted "merely because they chose in one form or another to exercise their democratic rights".[3] The investigation by the Victorian Ombudsman into these activities (and into the consequent

destruction of Special Branch files) resulted in the publication of five reports by the Ombudsman between 1984 and 1999;[4]

c. in 1984, *The Age* published articles disclosing the existence of illegal wiretaps by the New South Wales Police, leading to the Stewart Royal Commission which found (in 1986) that:

> From 1967 or 1968, over a period of some fifteen or sixteen years, a sophisticated system for the illegal interception of telephone conversation was developed within the NSW Police, introduced at the direction of the Commissioner of that police force. The existence of the system was known to and either expressly or tacitly approved by each succeeding Commissioner who held office prior to the present Commissioner. It was known to many senior officers and to many detectives. Officers of the Victoria Police knew of the system and were prepared to use it. Even members of the [Australian Federal Police] were prepared to use the system when the AFP's limited powers did not permit a particular interception to be made.[5]

d. in 1977, following pressure from the media and Parliament about whether secret police were engaging in political surveillance, the South Australian government commissioned a judicial inquiry by Acting Justice JM White, who concluded that South Australia Police's Special Branch had accumulated a great mass of irrelevant (often potentially harmful) material and that the Commissioner of Police had failed to inform the government of the existence of sensitive files on matters relating to politics, trade unions and other affairs, eventually leading to the dismissal of the SA Police Commissioner and the introduction of special instructions to limit the information police could collect.[6]

II. Privacy Concerns

Use of home entertainment & alarm systems for surveillance (clause 18)

7 Clause 11(3)(f) of the Model Bill authorises law enforcement agencies ("LEAs") to connect and operate a surveillance device ("SD") to a telephone system. During the JWG's inquiry, the Australian Federal Police ("AFP") submitted that a broader authority would be desirable to enable them to use other systems – such as data systems, alarm building monitoring and control systems, and home entertainment systems – to transmit information back to police. In its final report, the JWG concluded that it did not have sufficient time to consider the proposal and recommended further research or reform be done in this area.

8 The AFP's proposal has been taken up in the Commonwealth Bill. Once a SD warrant has been granted, clause 18(3)(f) allows LEAs to connect and operate a SD to a telephone system as well as to "any object or system that may be used to transmit information in any form".

9 If this is intended to allow LEAs to use home entertainment systems and the like to conduct surveillance, as is suggested in the JWG's report, then this is likely to have an impact on the extent to which the privacy of any person is affected – especially where such a system is located in a person's bedroom. In determining whether to grant a SD application, clause 16(2) requires the judge to consider any potential impact on a person's privacy. Clause 14(5)(5) of the Bill, however, merely requires LEAs to state the *kind* of SD that is sought to be used (eg, optical SD), not the *manner* in which the surveillance is to be carried out (eg, by using a home entertainment system). It is recommended that the SD application specify the system (if any) that is to be used to connect and operate a SD so that the judge can weigh the impact on privacy with greater precision.

Recommendation: Clause 14(5) of the Bill should be amended require an application for a surveillance devices warrant to specify any object or system that may be used [under clause 18(3)(f)] to transmit information in connection with the operation of a surveillance device.

Use of Surveillance Devices without Warrant (Part 4)

10 Part 4 (clauses 37-40) of the Commonwealth Bill sets out the authority for federal, State and Territory police to use optical, listening and tracking surveillance devices without warrant in the circumstances outlined below.[7]

11 Part 4 authorises warrantless surveillance in three respects:

a. clause 37 allows ***optical surveillance*** devices to be used without warrant if the use of the device does not involve:

   (i) entry onto premises (defined to mean land; building or vehicle, or any part thereof; and any place, whether built on or not – within or beyond Australia) without permission; or

   (ii) interference without permission with any vehicle or thing.

b. clause 38 authorises the use of ***any surveillance device to listen or record spoken words*** where the law enforcement officer is:

   (i) the speaker of the words, or the person (whether alone or in a group) to whom the words are spoken or by whom the speaker intends, or can reasonably expect, the words to be heard; or

   (ii) the law enforcement officer records or listens to words with the express or implied consent of a person who is permitted to listen to or record the words; and

c. clause 39 provides that ***tracking devices*** may be used with appropriate police authorisation, despite any State or Territory law forbidding the use of such a device without a warrant.

Surveillance, trespass & technology: Kyllo v. United States

12 The law of surveillance has traditionally been tied to the law of trespass and naked-eye surveillance. As was noted in *Kyllo v. United States*, [8] a recent United States Supreme Court decision involving the use of thermal imaging to detect heat lamps indicative of indoor marijuana growth but capable of detecting body heat, police are not expected to shield their eyes from looking at what is in plain view:

> The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment [prohibition against unreasonable search and seizure] jurisprudence was tied to common-law trespass…. Visual surveillance was unquestionably lawful because 'the eye cannot by the laws of England be guilty of a trespass.'…. We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property…, but the lawfulness of warrantless visual surveillance of a home has still been preserved. As we observed…, '[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.'

13 The court went on to acknowledge that technology enhances what might otherwise be ordinarily viewed, commenting that it then becomes a question of how much technological enhancement is too much. On the one hand, the court noted that people ought to expect some loss of privacy with advances in technology:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, …the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private.

14 On the other hand, in facing the question of what impact technology has on "the realm of guaranteed privacy", the court affirmed the need to maintain the test of "the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*". To abandon this test and allow for police to use sense-enhancing technology would, in the court's view, erode the privacy guaranteed under the Fourth Amendment.

15 While the matter before the court concerned police use of thermal imaging, the court noted that its views applied to other forms of surveillance that can be used by police without trespassing onto private land, such as powerful directional microphones and satellites. Foreshadowing the speed with which technology is developing, the court noted that it was important to ensure that the law takes into account "more sophisticated systems that are already in use or in development."

16 Judicial oversight is essential to ensure that police surveillance is restricted to what is necessary and proportionate in the circumstances. This was the position of the JWG who, when considering the proposal to allow police, rather than courts, to authorise surveillance:

> The JWG remains of the view that all surveillance warrants (and retrieval warrants) should be issued by a judicial officer. Given the intrusion of privacy involved in surveillance, it is necessary for an independent, impartial authority to evaluate the application and to consider whether surveillance is appropriate.

17 Judicial oversight over the use of intrusive powers of surveillance is critical because it:

a. ensures consideration is given to adopting less intrusive methods of investigation.

b. keeps the use of these intrusive powers to the necessary minimum;

c. maintains public confidence that the police imperative in favour of surveillance is balanced appropriately with the community's reasonable expectation of privacy; and

d. ensures appropriate accountability measures can operate.

Recommendation: Optical and tracking surveillance devices should only be used with appropriate judicial oversight.

Listening and recording spoken words without warrant

18 Clause 38 allows police to record conversations without warrant where they are a party to the conversation, the speaker can reasonably expect their words to be overheard, or police have the consent of one of the parties to listen or to record the conversation.

19 I refer the Committee to my submission to the JWG (attached), particularly paragraphs 43-47 (surveillance of non-"private" conversations); paragraphs 51-62 (participant monitoring); and paragraphs 63-67 (assistance to law enforcement agencies).

Recommendation: Surreptitious recording of conversations by or on behalf of police should only occur with appropriate judicial oversight.

Accountability

20 In addition to the loss of judicial oversight at the "front end" of the surveillance process (in allowing police to conduct surveillance without warrant, discussed above), the Bill has also departed from some of the "back end" (post-surveillance) accountability requirements for reporting and independent oversight.

Reporting back to court (clause 17)

21 Unlike clause 34 of the Model Bill, the Commonwealth Bill does not require the LEA to report back to the judge who issued the warrant. LEAs are instead required by clause 50 to make their report to the Minister.

22 One consequence of this is that, in exercising its "own motion" power to revoke a SD warrant under clause 17 of the Bill, the court is not assisted by any information on the manner in which the SD warrant has been implemented to date. The court is therefore not armed with any information that might alert it to the need to revoke a warrant that may have been improperly executed or inappropriately targeted. In contrast, clause 13(2) of the Model Bill specifies that this decision to revoke can be based on the report back to court.

Recommendation: LEAs should be required to report back to the judge, so that the judge can consider whether the surveillance device warrant should be revoked or other action taken.

Loss of accountability for warrantless surveillance

23 The safeguards and accountability provisions in the Bill only apply to situations where a warrant has been obtained. The provisions do not apply to warrantless surveillance. Consequently, surveillance conducted without warrant is not subject to the annual reporting obligations under Part 6, Division 2, including the LEA's obligations to:

a. report to the Minister in accordance with clause 49 on the conduct of each warrant and authorisation;

b. report to the Minister under clause 50 on the extent and effectiveness of surveillance and authorisation conducted over the year;

c. keep a register under clause 53 of warrants and authorisations sought.

24 This will impede the ability of the Ombudsman to conduct oversight of warrantless surveillance undertaken by police. Some kind of record seems to be a prerequisite to effective oversight if oversight is to occur after the fact. It will also make it impossible for Parliament and the community to know the extent of surveillance conducted by police without warrant.

Recommendation: The general conduct of any surveillance by police should be subject to independent oversight by the Ombudsman and the extent and effectiveness of its use be made known to the public through Parliament.

If Parliament nevertheless decides to permit warrantless surveillance, then the reporting requirements in Part 6, Division 2 should include a requirement to report on the use, extent and effectiveness of warrantless surveillance.

Destruction of surveillance records and reports (clause 46)

25 Clause 46 (based on clause 31 of the Model Bill) requires the destruction of surveillance records if they are no longer required for the permissible uses in clause 45.

26 In light of experience with creation and destruction of police records in other analogous contexts (Victorian Ombudsman's series of reports into Police Special Branch, 1984-1999; Stewart Royal Commission into illegal wiretaps by the New South Wales Police, 1984), it would be appropriate to allow for independent oversight of destruction decisions, for instance, by the Ombudsman. This would serve the dual purpose of ensuring that the surveillance itself was legitimate and that the destruction is actually carried out.

Recommendation: Clause 46 should be amended to require independent oversight (eg, by the Ombudsman) of any decision by police to destroy surveillance records, prior to their destruction.

PAUL CHADWICK
Victorian Privacy Commissioner
23 April 2004

Endnotes

[1] While the JWG, in its report, stated that it was not intended that the model surveillance provisions were not intended to authorise conduct that would otherwise be contrary to local privacy laws, this may not be achieved in a Commonwealth/State context.

[2] Keith Moor, "Police abuse home bugging", *Herald Sun*, 6 February 2003, available at http://www.heraldsun.news.com.au/printpage/0,5481,5942392,00.html, visited 28 April 2003.

[3] *Allegations Raised Concerning the Activities of the Operations Intelligence Unit and Other Related Issues*, second interim report of the Ombudsman, November 1998, page 91.

[4] The five reports by the Victorian Ombudsman are:

- *Destruction of Special Branch Files,* report of the Ombudsman, May 1984;
- *Report of the Ombudsman on Police Special Branch Documents*, March 1990;
- *Allegations Raised Concerning the Activities of the Operations Intelligence Unit and Other Related Issues*, interim report of the Ombudsman, May 1998;
- Allegations Raised Concerning the Activities of the Operations Intelligence Unit and Other Related Issues, second interim report of the Ombudsman, November 1998; and
- Allegations Raised Concerning the Activities of the Operations Intelligence Unit and Other Related Issues, final report of the Ombudsman, May 1999.

The May 1998 and May 1999 reports are available via the Ombudsman's website at http://www.ombudsman.vic.gov.au/pubs.html, visited 17 March 2003.

[5] Australia, *Royal Commission of Inquiry into Alleged Telephone Interceptions*, report of Mr Justice DG Stewart (Commissioner), 1986, para 16.11, Canberra: Australian Government Publishing Service. Discussed by P.N. Grabosky in "Telephone Tapping by the New South Wales Police" (1989) *Wayward Governance: Illegality and its Control in the Public Sector*, Chapter 3, Canberra: Australian Institute of Criminology, available at http://www.aic.gov.au/publications/lcj/wayward/index.html, visited 28 April 2003.

[6] South Australia, *Special Branch Security Records*, report of Mr Acting Justice JM White, 1977, Adelaide: Premier's Department. Discussed by P.N. Grabosky in "Political Surveillance and the South Australian Police" (1989) *Wayward Governance: Illegality and its Control in the Public Sector*, Chapter 7, Canberra: Australian Institute of Criminology, available at http://www.aic.gov.au/publications/lcj/wayward/index.html, visited 28 April 2003.

[7] It is noted, however, that clauses 37(2), 38(2) and 39(2) expressly state that these provisions do not authorise warrantless surveillance by State and Territory police where they are investigating "State offences with a federal aspect" (widely defined in section 3). The Explanatory Memorandum states that State or Territory police would need to use powers of their own jurisdiction in these instances.

[8] *Kyllo v. United States* 533 U.S. 277 (2001).