Submission to the Senate Legal and Constitutional Committee
The Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Bill 2005

The Council thanks the Committee for the invitation to comment on this Bill, and for the extension of time granted to prepare our response.

The Bill implements some of the changes recommended in the Sherman Report on named person warrants[1], and some other changes.

Introduction

i. The original Telecommunications (Interception) Act of 1979 permitted interceptions of telecommunications on very few grounds. There are now many. While justification might be claimed for some on the grounds that they help solve or prevent the most serious of crimes—murder, kidnap and those terrorism offences where life is at risk, for others (related for instance to the possession of child pornography, currency violations and tax evasion,) this is plainly not so. There has also been increase in the bodies that are permitted to obtain conduct surveillance. There is a slippery slope at work here.

This bill proposes to take us further down the slope, and in some cases, to remove the parliamentary brakes.

Each inclusion of new grounds for interception permits further invasion of the privacy of innocent persons. Each extension of the agencies permitted to intercept increases the likelihood of misuse. Proposals that can only be supported on the grounds that they are "important legislative tool[s] not available to enforcement agencies"[2] should be rejected.

ii. The number of warrants issued annually in Australia under the Telecommunications (Interception) Act (the TIA) has been increasing substantially, to the point where it exceeds the number issued for similar purposes in the United States of America. There are few refusals of requests for warrants, and none from any member of the Administrative Appeals Tribunal. There has been no significant increase in the number of such crimes reported, to justify this increase. Nor has there been a commensurate increase in criminal convictions of the most serious crimes.

It is a reasonable conclusion that interceptions are being authorised and undertaken for inadequate reason.

iii. The prime purpose of the TIA is to outlaw interceptions of telecommunications, not to create a large class of permitted interceptions. It is not just the privacy of those who are under investigation that is invaded whenever snooping powers are extended, but that of every person who contacts them, and of innocent persons using bugged telephones. Where there are

[1] Report of Review of Named Person Warrants and Other Matters, Commonwealth of Australia 2003
[2] Explanatory Memorandum to the bill.

alternative means of investigation of crimes which are less invasive and less productive of harm, those means should be preferred.

Details of the Bill

Schedule 1. The Criminal Code

This item permits the officers of certain agencies to use devices that hinder the normal operation of a carriage service, to modify or interfere with a device identifier (such as a SIM card), to possess items for the purpose of such modification, and to transmit or possess child pornography. The intention is to legalise the means to already existing powers of interception. In fact it permits further forms of interception.

It also permits an extension of the power to intercept to further, unspecified agencies, by way of regulation. No limit is set on what kinds of agencies may be included. The proposed subsection (k) should be deleted from the bill, and the power to determine the range of bodies given interception powers kept in hands of parliament.

The legitimacy for providing the means to intercept depends on the legitimacy of the provision of the powers to do so. There is ground for concern that the range of offences that the bodies investigate is determined by State acts, not acts of the Commonwealth.[3] An amendment to the NSW Crimes Commission Act, for example, would enable officers of the Crimes Commission to seek warrants in relation to crimes beyond its current concern with drug offences. As noted in the Introduction, there is reason to believe that such warrants would not be refused.

Recommendation 1: Subsection (k) of Schedule 1 should be deleted from the bill.

Recommendation 2: The Senate should implement a broader examination of the powers to intercept telecommunications.

Schedule 2. The Telecommunications (Interception) Act.

Items 1, 2, 3 and 4. Recording emergency communications.

These items replace an acceptable permission to record conversations without a warrant with one that is open to abuse.

The existing law (sections 6(2A) and 6(2B) of the TIA) permits the recording of communications over a telecommunications system to an emergency services number. Emergency service numbers are limited to telephone numbers on which assistance in emergencies may be sought from a police force, a fire service or an ambulance service, or one which is specified in regulations.

The TIA permits recording or listening to communication in these circumstances, without warrant and without warning to those communicating. It restricts this permission to persons who are lawfully engaged in duties relating to the receiving and handling of communications to an emergency services number.

[3] See subsection 5D (4) of the principal act.

The Bill replaces this arrangement as follows.

(i) The restriction to emergency telephone numbers is lifted. All telecommunications—by fax, email, web access, mobile, text message or telephone not connected with emergencies—may be recorded, without warrant or advice.

There may be point in recording a call to an emergency service, for vital information may be missed by the person taking the call. The justification given in the Second Reading Speech of the Minister for Justice for the proposed extension is that emergency services use hundreds of numbers behind the scenes in responding to a call. It is not clear to the CCL how recording all these calls will assist the provision of emergency aid. What might they hope to discover?

As the Senate Committee itself notes, this arrangement would permit the recording of personal pone calls and emails made by employees—a significant breach of privacy. This is not acceptable.

(ii) The restriction to persons handling communications to an emergency number as part of their duties is lifted. The intention is presumably to allow communications by other means than telephones to be included. Again, it is not clear what it is hoped will be gained. People do not report emergencies by text message or by email. Requests for emergency back-up might be sent by radio or mobile; but they are sent to dedicated receivers, lest they be lost in the general noise.

This proposal would allow a rogue police officer (a species that has been found in Australia) to intercept any conversation through a police station (or indeed to initiate and record one), evading the accountability procedures of the Act and subverting its principal intention, to outlaw interception.

In chapter 4 of his report, Mr. Sherman details a number of existing safeguards against illegal interception by such a rogue officer. However, most of the safeguards relate to the process of applying for warrants and keeping records, and so are irrelevant to the present difficulty. The remaining ones are that the rogue would need to be assisted by communications carriers, that arrangements for monitoring calls once interception is enabled would not permit undetected use, and that the consequences for an organisation of discovery of illegal phone tapping would be severe.

But if all the calls to an organisation were routinely monitored, the rogue would need no help. As for the consequences of discovery, Mr. Sherman himself reminds us that successive NSW Police Commissioners approved illegal interception of telephone conversations. Many police knew, in NSW, in Victoria and in the ACT. If rogue commissioners felt obliged to maintain such a widespread conspiracy for 15 years, agreement between lesser rogues can be anticipated. [4]

(iii) The only safeguard in the Bill is the restriction to emergency service facilities. But whereas the TIA requires emergency numbers to be listed in regulations, the Bill allows the Attorney General to declare in writing, any facility to be an emergency services facility.

[4] Paragraph 38

Further, the Attorney's declarations are not to be legislative instruments—there is no requirement for them to be made public, and it is clear that the intention is that they will not be. The Parliament will not have the power to over-ride them (save by fresh legislation).

There is nothing in the Bill to prevent a future (rogue) Attorney General from declaring all police premises emergency facilities. This is not fanciful. There have been some notable recent examples in democratic countries of politicians twisting meaning in order to evade legal restrictions.

It would not be difficult for an emergency service to restrict emergency traffic to a limited number of phone lines and radio frequencies.

Recommendation 3. That Item 1 of Schedule 2 be omitted from the Bill, and that item 3 be replaced by a clause restricting the recording of communications to those relating to an emergency current at the time of the call. The determination of premises should be restricted by reference to the kind of service provided.

Items 5, 6 & 7. Interference with radio communication.

The intended impact of this change, according to the Second Reading Speech, is to allow inspectors under the Australian Communications and Media Authority Act 2005 to intercept communications while investigating interference due to telecommunications services that use radio communication.

The CCL has no objection to this function. However, any information concerning the content of such material should be isolated from the provisions in the TIA that permit the use of legally obtained material for other purposes.

Item 8. Accessory after the fact.

The Bill extends the definition of 'class one offences' to include helping a person to escape punishment for, or to dispose of the proceeds of crimes of murder, kidnapping, narcotics offences, and a range of terrorism offences.

It is an example of the slippery slope: of a dubious extension of the powers to intercept, especially given the problems created by the definitions of terrorism offences, and some of the circumstances in which profits are made from a crime. While aiding and abetting a murder before the event creates an emergency, helping a person dispose of the profit on a map recklessly supplied to someone who turns out to be a member of a terrorist organisation does not.

Further, disposing of the proceeds of a crime is a complex area of law. It may be in the public interest for a book to be published about aspects of a genuinely serious crime; and a publisher might arrange for the proceeds to go to an innocent third party—a charity, say. A warrant should not be issued to tap the communications of the publisher.

The proposal that these offences be made class one (rather than class two) offences is not justified. There is no reason why a judge or an AAT member should be prevented from considering the gravity of an offence and privacy considerations before issuing a warrant allowing interception in relation to these offences.

We note as well our past objection to the introduction of terrorism offences when there are other crimes, such as that of murder, which cover the same wrongdoing.

Recommendation 4: that item 8 be deleted from the Bill.

Item 9. Civil Forfeiture.

This item is intended to implement recommendation 7 of the Sherman Report to allow the use of information obtained by lawful interceptions in proceedings by way of application for civil forfeiture. It does so by redefining 'proceeding for confiscation or forfeiture or for pecuniary penalty' permitting such information to be used in proceedings by way of application for a restraining order under acts to be prescribed. It is an example of the slippery slope at work.

i. The civil forfeiture acts are obnoxious. They enable persons to have their assets removed if it is held that it is more likely than not that they have committed a crime. These persons do not have to have been convicted of the crime. Instead, the acts are used where no conviction is possible, because the guilt of the accused person cannot be proved beyond reasonable doubt.

That is to say, a person is stripped of money or property **when there is still reasonable doubt about whether she/he is guilty**.

ii. Extraordinary powers are provided for the prevention of and the investigation of the most serious crimes. At the same time, safeguards in the criminal courts are there because the penalties attached to conviction are so serious. They apply, properly, not only to cases where a person may be deprived of liberty, but where substantial fines may be imposed. Without them, it is certain that innocent people will be found guilty.

The use of civil forfeiture acts evades these safeguards, for different procedures properly apply to (normal) civil cases. Further more, the NSW Act at least places an unreasonable burden on people to prove that their assets are not obtained with the use of funds originating from a crime. The extraordinary powers are not appropriate in relation to civil cases. The acts are an abuse of legal processes. The Commonwealth Parliament should not endorse them.

iii. The Senate should be slow to endorse the use of materials discovered in the investigation of one case as evidence in another. In the criminal justice system, what evidence may be used in court is carefully regulated. There are limits, for instance, on the use of what is found during a warranted search of a dwelling in prosecuting unrelated charges. An investigating officer may not hunt more broadly than is justified by the scope of the enquiry. He or she may not use a search warrant provided to investigate allegations of one crime (say a tax offence) as an excuse to hunt through unrelated parts of a dwelling. In part, the reason is to avoid discrimination and vicitimisation, such as might occur when an investigator has a prejudice against a minority group.

It is not so easy to regulate the abuse of electronic interception. An officer might install a Trojan horse, for example, and gain access to all the information contained a computer. The discovery of embarrassing material would provide the opportunity for and an incitement to

corruption. The more material found in the course of one investigation is able to be used in different cases, the more the temptation for an investigating officer to extend his or her search.

iv. The CCL is also concerned that the manner of determining which acts are prescribed is to be by regulation. It would be better for amendments to have to be made by a fresh act. But if acts are to be prescribed by regulation, the Bill should be amended to make this explicit.

v. As with the proposed change in Schedule 1, there is concern about future changes to the State Acts. In the NSW Act, for instance, there are safeguards of the right of a respondent to use part of what is alleged to be the proceeds of a crime for the purposes legal costs connected with his/her defence. That right might be removed. Or the State might decide to include debt recovery in its act. Here the Commonwealth loses control over its descent of the slippery slope.

Recommendation 5: That Item 9 be rejected.

Items 10, 12 and 14. New requirements for reporting.

The CCL welcomes the amplification of the requirements on the ombudsman to report the biannual inspections if agencies' records, and those introduced by items 12 and 14, for agencies to report annual statistics of the applications for named person warrants and the number of services they involve, and also for the statistics concerning the effectiveness of those warrants.

We are concerned however that recommendation 5 of the Sherman report is not being implemented. Accountability procedures for ASIO are particularly important, given both its past history and the necessary secrecy under which it operates. ASIO is not being asked to reveal its targets, nor how many they are, not to indicate what kinds of interceptions it uses, nor anything else about its methodology.[5]

Such limited reporting would not enable any target person or organisation to take counter-measures.

CCL also supports the second part of Sherman's Recommendation 5, that the number of warrants refused be published. This is important information, not only for ASIO's accountability, but also for its reputation, and the confidence with which citizens can support it.

Recommendation 6: the Senate Committee should propose an amendment to the Bill, inserting the requirements that ASIO report publicly on the number of telecommunication intercept warrants and named person warrants applied for, refused and issued in the relevant reporting year.

The CCL also objects strongly to the rejection of Sherman's recommendation 8, that the definition of 'restricted record' be restored to its form prior to the amendment to the TIA in 2000. That definition read "'restricted record' means a record obtained by means of an

[5] Cf. the remarks of the Director-General quoted in the Sherman Report at paragraph 206. The Inspector General of Intelligence Services supported the Sherman proposal as Sherman notes in paragraph 213.

interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system." The present act restricts the definition to the original, excluding copies.

Legislation that restricts keeping records of originals of interceptions but permits the keeping of copies is ill-conceived. All the reasons that apply to restricting the availability of originals apply also to copies.

It is true that some forms of copying are difficult to police. But that does not mean that they should be legalised.

Recommendation 7: that the definition of 'restricted record' be restored to its form prior to the amendment to the TIA in 2000.