
Part 3

1.57 This Part creates a new regime of civil remedies for unlawfully intercepted material in addition to criminal penalties in the Principal Act and under any other Commonwealth or State law. Mr Pat Barrett made a recommendation to the effect that "a right of action against a person who unlawfully intercepts or publishes a telephone communication should be conferred on the person whose communication is unlawfully intercepted."¹⁵

1.58 The civil remedies which the Part proposes require an 'aggrieved person' to be a party to a communication or have the communication made on their behalf. The defendant needs to intercept the communication or be complicit in an interception. The civil remedy proposed by the Bill is very wide and empowers the Court to make any such orders against the defendant as the Court considers appropriate.

1.59 The proposed subsection 107A(7) "without limiting the orders that may be made under this section" lists some of the kinds of orders that a court might make. These are:

- (a) declarations that the interception was unlawful;
- (b) an order for damages;
- (c) an order in the nature of an injunction;
- (d) an order by way of restitution or as the Bill states an order that the defendant pay to the aggrieved person an amount which represents "in the opinion of the court, the total gross income derived by the defendant as a result of the interception or communication, as the case requires."

1.60 The proposed subsection 107A(8) explicitly states that the court in assessing damages may award punitive damages.

1.61 It is contemplated that this jurisdiction will be exercised by the Federal Court of Australia or "a court of a State or Territory." The proposed subsection 107A(5) further contemplates ancillary civil relief for a victim in criminal proceedings. The proposed subsection seeks to allow an aggrieved person to use the criminal proceedings under section 7 of

¹⁵ Ibid at p16.

the Principal Act as a means to base civil proceedings against the defendant. The explanatory memorandum states:

"As the same conduct may found civil liability as well as the criminal liability, this provision saves an aggrieved person from having to present the same evidence again in a civil court."

The section appears to contemplate that civil proceedings will be 'tacked on' to the criminal proceedings, the same court handling both.

1.62 These civil remedies will bind the crown.¹⁶

1.63 The Committee did not receive any adverse evidence concerning the proposed civil remedy although Mr Kevin O'Connor did raise an important issue concerning how an individual might become aware of a possible cause of action.

"On the question of the civil remedy, it is an important advance, and I have indicated that. The Barrett report favoured a view that I have certainly put forward on other occasions that, if a warrant does not lead to criminal prosecution, the existence of that interception ought— I believe—to be notified at some point to the subjects of the interception and the warrant. The Barrett report is striking on this matter, at pages 71 and 72 of the public document, where it considers the police objections, the culture of secrecy which understandably surrounds police operations in respect of criminal investigations, and their concerns about dealing with people in this way.

Two major policing nations with whom we often compare ourselves—Canada and the US—do this. As I read the Barrett report, they are untroubled by the proposition that, at some point in the process of secret surveillance, people should be made aware of what has occurred. That is really the best antidote to improper activity, and is really made manifest tonight by these protestations from people about the

¹⁶ Section 4.

maintenance monitoring that they feel was unfairly undertaken. They became aware of it, and they have acted to defend their rights..... it seems to me that the civil remedy will only be a measure of protection for those who somehow find out that this kind of interception has gone on. So you have this strange situation where the person against whom the warrant information is used in a trial will find out that the person who is not brought to trial will not find out. It could be argued that the person who is possibly more culpable gets an opportunity to use a civil remedy while the person who is less culpable does not. I think that is a dilemma that will need to be addressed."¹⁷

Part 4

1.64 This part of the Bill prohibits the disclosure of information about applications for warrants, their existence and details concerning a warrant. The proposed section 6EA defines 'designated warrant information' as:

"(a) information about any of the following:

- (i) an application for a warrant;
- (ii) the issue of a warrant;
- (iii) the existence or non-existence of a warrant;
- (iv) the expiry of a warrant; or

(b) any other information that is likely to enable the identification of:

- (i) the telecommunications service to which the warrant relates; or
- (ii) a person specified in a warrant as a person using or likely to use the telecommunications service to which the warrant relates."

1.65 The Bill will criminalise the disclosure of 'designated warrant information' by amending section 63. In accordance with section 105, which criminalises breaches of the Principal Act generally, disclosing warrant information will carry a penalty of \$5000 or 2 years in gaol.

¹⁷ Evidence L&C (21 March 1995) 447.

1.66 The proposed section 63AA creates some exceptions to the prohibitions. These primarily relate to the application process, issue of warrants, record keeping and reporting requirements of the Principal Act. In each of these cases there is a practical necessity for warrant information to be disclosed.

1.67 This provision comes from one of Mr Pat Barrett's recommendations (No.9) and faithfully follows its intent which was that the Principal Act "should be amended to prohibit the disclosure of the existence of a warrant other than in accordance with that Act."¹⁸ The ostensible justification for this recommendation was that there was uncertainty as to whether the *Freedom of Information Act* applies to Telecom and specifically to warrant information. The prohibition was considered necessary to secure the privacy of individuals subject to telephone interception.¹⁹

1.68 The Committee heard no strongly adverse evidence concerning this provision of the Bill. The Committee believes that provision will greater enhance the protection of individual privacy afforded by the Principal Act and is therefore a desirable measure.

Part 5

1.69 This part expands the existing reporting obligations²⁰ in response to Recommendation No. 13 of the Barrett report which stated that:

"In their reports on the execution of particular warrants, agencies should be required to include an assessment of how useful the information was and whether it led to an arrest or is likely to do so."²¹

¹⁸ Barrett Report p16.

¹⁹Ibid p.64.

²⁰ Section 94 requires that the chief officer of Commonwealth agencies using intercept facilities report to the Attorney General after each warrant is issued and "as soon as practicable after" revocation as to the use made of information obtained and to whom it is communicated. Section 96 requires eligible state authorities to report yearly.

²¹ Recommendation 13 Barrett report at p.18.

1.70 The new reporting obligations will require that information detailing the number of arrests made or likely to be made on the basis of the warrant information and an assessment of the usefulness of the information be included [proposed subsection 94(2)]. Part 5 also contains two formulae: one for giving some indication of the efficacy of interception [proposed subsection 102(3)]; and another for some measure of its cost effectiveness [proposed subsection 103(aa)]. In both cases the information needs to be communicated to the Attorney with other reporting information.

1.71 The submission of the Law Society of New South Wales criticises this section on the ground that it should contain more detail. Mr Maurie Stack, President of the NSW Law Society, noted that the reports would not assess the social and economic effects of the intercept.²² The Law Society includes in its submission an alternative reporting format, modelled on American and Canadian practice, which includes notification of persons who have had their phones intercepted.²³

1.72 The provision nevertheless was strongly supported by Ms Beverly Schurr, New South Wales Council for Civil Liberties, in her evidence before the Committee:

"We welcome the proposal to require, for the first time, some sort of costing information to be provided. In the past, the government has been embarrassed about the inability to provide definite financial costs for phone tapping."²⁴

1.73 The Committee believes that these provisions are a desirable expansion in the mandatory information required to be communicated to the Minister and will, if enacted, provide a useful measure of the efficacy of telecommunications interception.

²²Submission 8 at p2.

²³ Barrett Report at p18.

²⁴ Evidence L&C (212 March 1995) 442.

Part 6

1.74 This part deals with interception by carriers and is in direct response to the concerns raised by the CoT cases and the inquiry conducted into their complaints by Austel.

1.75 The proposed paragraph 7(2)(a) seeks to tighten up the existing exemptions which allow employees of a carrier to lawfully intercept a communication by adding the element of necessity. The structure of the existing exemption is preserved, although the carrier will, under the proposed amendments, need to show that interception is "reasonable necessary" to do an act or thing in order to perform those duties effectively.

1.76 A new paragraph 7(2)(aa) will place a similar limitation on the authority of independent contractors to intercept telecommunications lawfully.

1.77 The proposed subsection 7(2) of the Bill directs a court when deciding whether an interception was "reasonable necessary" to have regard "to such matters as are specified in, or ascertained in accordance with, the regulations."

1.78 Mr David Krasnostein, General Counsel, Telecom Australia, in his submission to the inquiry²⁵ criticised these amendments on a number of grounds. His principal objections are that the Bill seeks to impose restraints on interceptions in a way which is prejudicial and unfair to Telstra and its employees by exposing them to unreasonable risks of prosecution for criminal offences. This difficulty arises due to the inserted criterion of 'reasonable necessity'.

1.79 Telecom\Telstra in their submission proposed an amendment to the proposed subsection 7(2A). Their proposed amendment would read as follows:

"7(2A) For the purpose of paragraphs (2)(a) and (aa), in determining whether an act or thing done by a person was reasonably necessary:

²⁵ Sub. 10.

(a) a court is to have regard to such matters as are specified in, or ascertained in accordance with, the regulations; and

(b) any act or thing done by a person in good faith in compliance or purported compliance with matters (including guidelines or procedures) specified in, or ascertained in accordance with, the regulations, will be taken to be reasonably necessary²⁶

1.80 The concern raised by Telcom was echoed by a number of witnesses who gave evidence before the Committee. Ms Milligan, Industrial Officer, CEPU²⁷, stated in her evidence that:

"The union is concerned about the legislation. In fact, we are extremely alarmed by the proposed amendments to section 7(2) of the legislation. Our view of that part of the bill is that it imposes an unreasonable and exceptionally vague test to determine the individual civil liability under the new and very wide ranging civil liabilities proposed by the Act. On our understanding that is the new imposition of the Act which has a primary significance for our members who are involved in implementing the interception procedures.

The union is specifically concerned about the situation where an employee who is acting in good faith and in strict compliance with any guidelines, or regulations which flow from the Act, may still be found by a court of law to be open to civil prosecution for their actions. We are very concerned about that situation. We believe that an employee in those circumstances should be specifically protected by the Act. I refer to the test provided for in the amendment - which will be considered by a court—that the action was reasonably necessary in order to perform the person's duties effectively. That is open to a court to review. As I understand the

²⁶ Sub. 10 p3.

²⁷ The full name of this organisation is the Communications, Electrical, Electronic, Energy, Information, Postal, Plumbing and Allied Services Union of Australia.

amendment, the court is directed to have reference or regard to the guidelines and regulations. But strict compliance with those guidelines and regulations is not by any means a complete defence for that employee. The employee's acts can be reviewed, and determined to be not in compliance with that test by a court of law even though the employee has done everything they possibly can do to conform with every piece of information and guideline that they have been given.

In the union's view, a complete defence in those circumstances should be made available to the employee concerned: that is, the employee carrying out their ordinary duties in an authorised manner. To this end having had the advantage of examining the submission put forward by Telstra to the committee, given the obvious sensitivity our organisation would have, we would say that we support the proposal put forward by Telstra to amend the bill at that section, section 7(2). That in our view is a critical area. Even though it is patently obvious that the prime target for such civil litigation would be the corporation, nevertheless the individual employee is open for that action. That in itself, we believe, will, at the very minimum, create extraordinary disruption to routine day-to-day activities which employees are required to carry out.

Our view is that this protection must be explicitly provided for in the bill in at least the form put forward in the submission by Telstra. Without that being taken into account in that manner, we would strongly object to the bill going forward, and we believe it is severely flawed."²⁸

1.81 Mr Ross Ramsay, Optus, voiced concern over the proposed amendments to section 7 and also suggested that greater reliance should be placed on internal guidelines.²⁹

1.82 A number of the CoT cases present at the Committee's hearing on 21 March expressed concern that the present amendments did

²⁸ Evidence L&C (21 March 1995) 436.

²⁹ Evidence L&C (21 March 1995) 450.

not go far enough in tightening up the carrier exception. Mr Graham Schorer, spokesperson, CoT cases, stated in his evidence that:

"Yes, the Senate does have a role, not only to individuals but to corporations. Everyone is going to be using the telecommunications system on this information highway. It is as open as a can of worms. But this legislation is not addressing it, because it is not going to allow the evidence to be collected to bring about the charges to stop it happening. And the individual people within Telecom are not given any encouragement to come forward on their fellow people who are doing it on their own, or are wrongly accepting instructions from those above. I believe that if there is a genuine need for proper monitoring, listening or taping of a conversation or a service, because they can do both, it should not be a matter of the telecommunications people going along to the person. If they are going to get prior written consent, they should apply to the regulator, Austel, and justify to Austel why this particular identification of fault requires this treatment. I certainly do not accept that this sort of treatment of listening and taping and monitoring is part of network maintenance. That is a lot of codswallop. Ask any technical communications consultant."³⁰

1.83 Mr Kevin O'Connor, Privacy Commissioner, in his evidence before the Committee stated that:

" On the final question of maintenance, I put forward the view in correspondence with the department that I think the proposition of obtaining consent for all recording should at least be more actively canvassed. As I understand it, what we have at the moment is that consent is to be obtained if the recording occurs in response to a complaint but consent is not necessary if it is being undertaken for maintenance purposes in accordance with the guidelines. I would argue that, if you are going to go as far as recording, it may be appropriate that consent be obtained or possibly you can put a quantitative limit on it—for example, recording of a certain duration or of

³⁰ Evidence L&C (21 March 1995) 435.

a certain extent should be subject to consent.

I think there are difficulties with going that far in respect of this incidental listening and that kind of thing. I accept from what I have been told over the years by Telecom that it is inevitable in the maintenance environment that some form of listening into the lines to assess the quality of communications is necessary. I am interested in this shift from mere listening, with the risks that has in terms of redisclosure of information, and actual recording."³¹

1.84 The Committee received a submission from Mr Warwick Smith, Telecommunications Industry Ombudsman, which contained a copy of Telecom's internal '*Guidelines on Voice Monitoring or Recording of Telephone Services*'. These guidelines were drafted in response to the CoT cases saga and have been adopted by Optus and Vodaphone. They appear to be establishing themselves as the industry standard. These guidelines, for example, provide that where extended voice monitoring takes place it should only occur with the consent of the customer. A copy of these guidelines is annexed to this report at appendix 3.

1.85 In his brief submission Mr Smith supported the 'reasonableness' test but suggested that it should be strengthened by linking it with an appropriate industry code such as Telecom's internal guidelines.³²

1.86 The Committee was fortunate in its inquiry to have the assistance of Mr Michael Rozenes QC, Commonwealth Director of Public Prosecutions. The Committee heard whether the recent decision by the DPP not to charge a Telecom employee was due to a technical deficiency of the Principal Act and whether the amendments in the Bill would assist in curing any such deficiency:

" **Senator ABETZ**—As I understand it, the question that we basically wanted to ask was on the concern expressed at the last hearing that the employees of Telecom allegedly could not be charged. That is, I think, what we were advised by Mr

³¹ Evidence L&C (21 March 1995) 447.

³² Sub.7 p3.

Reaburn. We as a committee want to know, firstly, whether that was the case; and, secondly, whether this new bill will overcome what some people see as a deficiency.

Mr Rozenes—There was no prohibition on them being charged, there was just no likelihood of us recommending that course, because there was no satisfaction on my part that there were reasonable prospects of securing a conviction on the evidence then available. Were there to be admissible evidence that could have resulted in a conviction, there would have been no reason why Telecom employees could not be charged under the existing legislation.

Senator ABETZ—So it was only an evidentiary problem, as you saw it, as opposed to a technical problem with the legislation.

Mr Rozenes—Yes. There is nothing wrong with the legislation, in that it goes just so far but no further. But in attempting to obtain a conviction on the sort of evidence that one expects to get in such cases, there is no high chance of success.

Senator ABETZ—So getting a successful prosecution in any case would be difficult, given the framing of the legislation?

Mr Rozenes—I would say it would be difficult in this sort of case; and I do not see that it would be any easier under your proposed legislation, either.³³

1.87 There was also discussion of a letter, dated 2 March 1995, from Mr Rozenes, tabled by Mr Robert Bray, concerning the DPP's decision not to prosecute a Telecom employee in Ballarat. In evidence before the Committee the following exchange occurred:

" **Senator SPINDLER**—I have got a question that relates to a letter that the committee received and that has been tabled. In the letter you state, Mr Rozenes, that you are not proceeding with prosecutions because as a result of legislative

³³ Evidence L&C (27 March 1995) 495.

changes made in 1991, and I quote: *Telecom employees are no longer officers of the Commonwealth for the purpose of the Crimes Act 1914.*

Mr Rozenes—That decision is the subject of a further review by my office at the very moment that we speak.

Senator SPINDLER—I see. I was just wondering whether you thought that it might be necessary, seeing that we are talking of an area that is of considerable importance in the community, that we should either seek amendments to the Crimes Act or somehow have an amendment in the telecommunications legislation to cater for this situation.

Mr Rozenes— I think there may be some legislation that is currently available that my office overlooked in the course of determining this matter in the first place; and as I say, that is the subject of further consideration.³⁴

1.88 The Committee believes that the amendments contained in this part are an improvement on the present situation. The Committee nevertheless believes that they cannot stand alone and need to be supported by appropriate regulations. The proposed subsection 7(2A), in part, provides such a vehicle. The proposed subsection reads:

"(2A) For the purpose of paragraph (2)(a) and (aa), in determining whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertainable in accordance with, the regulations."

1.89 Telecom's internal '*Guidelines on Voice Monitoring or Recording of Telephone Services*' appear to the Committee to provide a potentially ready made model for regulations. The Committee believes that in view of the fact that an industry standard appears to have emerged, consideration should be given to making Telecom's internal guidelines, at least, the starting point for regulations. While the linkage

³⁴ Evidence L&C (27 March 1995) 497.

would not be as strong as that proposed by the Telstra amendment the Committee nevertheless believes that the giving of legal stature to the guidelines would allay the fears of both the union and industry groups concerning lack of clarity in what would be 'reasonably necessary' whilst increasing the protection afforded to individual privacy.

Schedule 2

1.90 This schedule amends the *Telecommunications Act*. The primary effect of these amendments is to make it a licence condition that Telecommunication carriers pay for the development of an 'interception capacity' (for law enforcement and intelligence related intercepts) on their lines. The amendments also provide that the carrier will be able to seek to recover those costs, over time, from the other party or parties [proposes subsection 72A(6)]. Nevertheless in the initial creation of an interception capability this will be borne by the carrier [proposed subsection 73A(5)].

1.91 This implements recommendations Nos 14 and 16 of the Barrett report.³⁵ Mr Pat Barrett explicitly recommended that carriers have the capacity to recover the costs of maintaining interception capabilities from users. His rationale for such an arrangement was that:

"In keeping with the commercial orientation of the arrangements, each agency (Commonwealth or State) would contract with the relevant carrier on the basis of its individual access to the capabilities. There would be a discipline on all agencies to indicate an interest or otherwise quickly so that they could make their own cost effectiveness. There would clearly be an incentive to maximise participation to minimise cost. Moreover, it would be a real test of the collective view of the value and priority of the capability."³⁶

1.92 Mr Pat Barrett, in his review, canvassed an option that

³⁵ at p 20.

³⁶Barrett Report p105.

carriers only be able to recover the capital costs, but not interest, associated with the establishment of telecommunications interception facilities from agencies.³⁷ The proposed regime in schedule 2 contemplates that carriers are able to recover "the costs (whether of a capital nature or otherwise) relating to the creation or development of the interception capability." This appears broader than mere capital costs, although seems to fall short of allowing a carrier to recover all the running costs associated with maintaining an interception facility.

1.93 The Bill does not differentiate between State and Commonwealth agencies, although during the Committee's inquiry it was the State agencies who voiced concern over the introduction of an element of 'user pays'. Mr Mick Williams, Detective Chief Inspector, Victorian Police stated in his evidence before the Committee that:

"From a funding perspective, the Victoria Police are strongly opposed to the proposed amendment requiring carriers to fund interception capabilities and then recover the costs from the agencies. In our original submission we asserted that the development of interception services should be funded by carriers, and that they should in fact be recovered from subscribers. We still strongly maintain that view. There may be some who assert that under such a concept of carrier pays and recovers from subscribers, law enforcement agencies may well say that we want everything made interceptible. That is not so. In fact, a precedent has already been set under the revamped Austel new technology subcommittee, where the agencies have opted to accept interception measures that are of a lesser standard. We refer to them as interim interception measures. There have been some instances where we have said that we do not need services that are about to be released to be interceptible. We are saying that the situation will not occur where we will ask for everything to be interceptible. Some may say there will be a greater use of telephone interception. We very, very strongly reject that. As I have already alluded to, the existing stringent legislation prevents us from going on any fishing expedition or anything

³⁷ Ibid p 103.

like that. The legislation does not allow us to misuse it, so we reject that assertion."³⁸

1.94 Mr Phillip Bradley, New South Wales Crime Commission, also voiced similar concerns in relation to the funding implications of the Bill.³⁹

1.95 Mr Ross Ramsay, Manager, Government Liaison, Optus, expressed concern in his evidence before the committee over a suggestion that carriers should be made to pay the cost of the development and maintenance of telecommunications interception capabilities:

"I would like now to turn to another matter, raised by Mr Bradley's intervention earlier on funding. What I think Mr Bradley said was that the funding ought to be by the carriers for capital matters— I assumed it was capital matters— and that this should just find its way into customer prices. I would like to comment that there is a need for discipline on both sides of the house where funding is concerned. There are many levels of interception capability, not just one. It is not one simple matter. Some levels of interception capabilities are more costly than others, so agencies need to decide what level of interception capability is appropriate for the task, and know the cost involved and be prepared to participate in the funding."⁴⁰

1.96 After this evidence was heard on 21 March 1995 the Committee received a submission from Mr Pat Barrett, Deputy Secretary, Department of Finance. In his submission Mr Barrett stated that:

"In relation to state funding, while Ross Ramsay (Optus) raised the important question as to who should pay, the issue of charging also involves pragmatic questions about the nature and timing of significant expenditure on TI, such as for GSM and the move to digital technology on the network.

³⁸Evidence L&C (21 March 1995) 418.

³⁹ Evidence L&C (21 March 1995) 421.

⁴⁰ Evidence L&C (21 March 1995) 450.

Having to fund such decisions, really requires an assessment by the various Agencies as to the benefits likely to be derived in the current environment and in relation to other priorities.

To the extent that Federal Agencies such as ASIO require interception capability sooner than State Agencies, the former bear the brunt of the initial expenditure. The State Agencies only pay when they use the capabilities. As well given the cost, the coordination mechanism provided by LEAC ('the Law Enforcement Advisory Committee') requires a disciplined assessment of the capability required and more particularly when it is required."⁴¹

1.97 The Committee believes that the cost discipline which the proposed amendments will produce is desirable. This is especially the case with the proliferation of new technologies where the introduction of a cost element will force agencies to prioritise their interception needs so as to avoid an excessive burden being placed on the carriers and ultimately the subscribers to any system.

⁴¹ Sub 19 at p1.

Conclusions

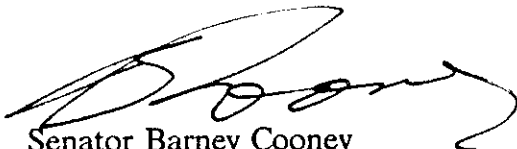
1.98 Mr Kevin O'Connor stated in his evidence before the Committee that:

"The bill is, I think, a careful attempt to bring an increased level of discipline into various aspects of the process that surrounds the obtaining of telecommunications interception warrants and, obviously, I welcome the elements of the bill that seek to incorporate greater scrutiny into the process of the effectiveness of warrants, in particular, and the cost of warrants. The reference in the bill to a civil remedy is not unimportant and is a significant new acknowledgment of the importance of the parliament protecting individual privacy interests through more accessible mechanisms than had previously existed."⁴²

The Committee agrees with these sentiments and is satisfied that the measures contained in the Bill are necessary and should be enacted into law.

Recommendations

Recommendation: A majority of the Committee recommends that the Bill as introduced be enacted.



Senator Barney Cooney
Chair

⁴² Evidence L&C (21 March 1995) 445.